

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:

Jun OGAWA

Application No.: To be Assigned

Group Art Unit: To be Assigned

Filed: February 19, 2004

Examiner: To be Assigned

For: NAME/ADDRESS TRANSLATION DEVICE

**SUBMISSION OF CERTIFIED COPY OF PRIOR FOREIGN
APPLICATION IN ACCORDANCE
WITH THE REQUIREMENTS OF 37 C.F.R. § 1.55**

Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Sir:

In accordance with the provisions of 37 C.F.R. § 1.55, the applicant(s) submit(s) herewith a certified copy of the following foreign application:

Japanese Patent Application No(s). 2003-091293


Filed: March 28, 2003

It is respectfully requested that the applicant(s) be given the benefit of the foreign filing date(s) as evidenced by the certified papers attached hereto, in accordance with the requirements of 35 U.S.C. § 119.

Respectfully submitted,

STAAS & HALSEY LLP

Date: Feb. 19, 2004

By: 
Gene M. Garner II
Registration No. 34,172

1201 New York Ave, N.W., Suite 700
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501

Op 1723

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 3 年 3 月 2 8 日
Date of Application:

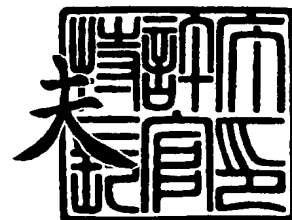
出 願 番 号 特 願 2 0 0 3 - 0 9 1 2 9 3
Application Number:
[ST. 10/C]: [J P 2 0 0 3 - 0 9 1 2 9 3]

出 願 人 富 士 通 株 式 会 社
Applicant(s):

2 0 0 3 年 1 1 月 2 7 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康 夫



出証番号 出証特 2 0 0 3 - 3 0 9 8 3 0 3

【書類名】 特許願

【整理番号】 0252577

【提出日】 平成15年 3月28日

【あて先】 特許庁長官殿

【国際特許分類】 H04L 12/00

【発明の名称】 名前／アドレス変換装置

【請求項の数】 5

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号 富士通株式会社内

【氏名】 小川 淳

【特許出願人】

【識別番号】 000005223

【氏名又は名称】 富士通株式会社

【代理人】

【識別番号】 100089244

【弁理士】

【氏名又は名称】 遠山 勉

【選任した代理人】

【識別番号】 100090516

【弁理士】

【氏名又は名称】 松倉 秀実

【連絡先】 0 3 - 3 6 6 9 - 6 5 7 1

【手数料の表示】

【予納台帳番号】 012092

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9705606

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 名前／アドレス変換装置

【特許請求の範囲】

【請求項 1】

通信元から送信される、通信先の名前に対応するアドレスの問合せを受信した場合に、通信元及び通信先がそれぞれ属するネットワーク種別に基づいて、通信元と通信先との間の通信の可否を判定する判定手段と、

前記判定手段の判定結果に基づいて、前記名前に対応する通信先のアドレスを通信元に回答するか否かを判定する第 2 判定手段と、

前記第 2 判定手段が通信先のアドレスを回答すると判定した場合に、通信先のアドレスを取得して通信元に回答する回答手段と、
を含む名前／アドレス変換装置。

【請求項 2】

第 1 ネットワーク及び第 2 ネットワークから送信される、通信先の名前に対応する通信先のアドレスの問合せを受信する受信手段と、

前記問合せを送信した通信元、及び前記通信先がそれぞれ属するネットワークを識別する識別手段と、

前記通信元が前記第 1 ネットワークに属し且つ前記通信先が前記第 2 ネットワークに属する場合には、前記通信元に対して回答すべき前記通信先のアドレスを検索する検索手段と、

前記通信先のアドレスを含む回答を送出する送出手段とを含み、

前記送出手段は、前記通信元が前記第 2 ネットワークに属し且つ前記通信先が前記第 1 ネットワークに属する場合には、前記通信先のアドレスを含む回答を送出しない

名前／アドレス変換装置。

【請求項 3】

前記送出手段は、前記第 1 ネットワークに属する通信元と前記第 2 ネットワークに属する通信先との間での通信で使用が許可されたアプリケーションがない場合には、前記通信元へ前記通信先のアドレスを回答しない

請求項 2 記載の名称／アドレス変換装置。

【請求項 4】

前記第 1 ネットワークに属する通信元に相当する第 1 端末に対して前記第 2 ネットワークに属する通信先に相当する第 2 端末のアドレスが回答される場合に、前記第 1 ネットワークと前記第 2 ネットワークとの間を転送されるデータを受信して通過が許可されたデータのみを通過させるとともに、前記第 1 ネットワークと前記第 2 ネットワークとの間のアドレス変換を行う中継装置に対し、前記第 1 端末と前記第 2 端末との間を転送されるデータを通過させるための通過情報を通知する通知手段をさらに含む

請求項 2 又は 3 記載の名称／アドレス変換装置。

【請求項 5】

前記通知手段は、前記中継装置が前記第 2 端末から送信されるデータを通過させるときに、このデータに送信元アドレスとして付加された前記第 2 端末の前記第 2 ネットワークにおけるアドレスを前記第 1 ネットワークのアドレスに変換するために、前記第 2 端末に対して仮想的に割り当てられる前記第 1 ネットワークのアドレスと前記第 2 端末の前記第 2 ネットワークにおけるアドレスとを含む通過情報とを前記中継装置に通知し、

前記送出手段は、前記第 1 端末が前記第 2 端末宛のデータに前記第 2 端末の前記第 1 ネットワークにおけるアドレスを送信先アドレスとして付加して送信し、且つ前記中継装置が前記第 2 端末宛のデータを通過させるときにこのデータに付加された送信先アドレスを前記第 2 端末の前記第 2 ネットワークにおけるアドレスに変換するために、前記第 2 端末の前記第 1 ネットワークにおけるアドレスを含む回答を送出する

請求項 4 記載の名称／アドレス変換装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、IP ネットワーク間における通信確立時のネゴシエーションに関する。

【0002】

【従来の技術】

従来、IP (Internet Protocol) 通信に関連する技術としては、以下のよう
なものがある。

【0003】

(1) 名前解決

IP 通信を行う場合には通信元 (問合せ元) 端末のユーザは、一般的に通信先
(問合せ先) をホスト名で指定する。このホスト名を IP アドレスに変換するた
めに DNS (Domain Name System) が用いられている。DNS は、TCP/IP
ネットワーク環境において、通信先 (問合せ先) のホスト名 (ドメイン名) から
、対応する IP アドレスを取得できるようにするサービス、即ち「名前解決」を
提供するシステムである。DNS サーバは、ホスト名と IP アドレスの対応関係
を記述したデータベースを管理しており、クライアントからの要求に応じて、ホ
スト名からその IP アドレスを参照できるように機能する。これにより、ユーザ
は、憶えにくく、分かりにくい IP アドレスではなく、ホスト名を指定してネッ
トワークにアクセスすることができる。DNS の実体は分散データベースであり
、図 1 に示すような、ドメイン・ツリーと呼ばれる構成により、膨大な数の名前
と IP アドレスの解決を実現している。

【0004】

図 1 に示されるように、ドメイン・ツリーにおいて、各ノードに位置する DN
S サーバは、基本的に、自身の管理するドメイン内情報とサブドメインの DNS
サーバ名しか知らない。そのため、DNS への問合せ側は、ホスト名を元にこの
階層を上位から順にたどっていけば、最終的に IP アドレス (図 1 では「www. fo
rum. atmark. co. jp」の IP アドレス “192. X. X. X”) を知る DNS サーバまでた
どり着くことができる。以上のような手法により、IP 通信では名前解決を実現
している。

【0005】

(2) IP アドレスの種別とアドレス変換技術

IP アドレスには、その割当てポリシーから「グローバル IP アドレス」と「

「プライベート IP アドレス」の二種類のアドレス空間が定義されている。グローバル IP アドレスは、インターネットで使うことを許された IP アドレスである。プライベート IP アドレス (RFC1918で規定) は、常時外部 (Internet) への接続が必要ではない組織内部のネットワークアドレスとして自由に利用できる IP アドレスである。

【0006】

この二種類の IP アドレスがそれぞれ定義されているプライベート IP アドレス空間とグローバル IP アドレス空間にまたがる通信では、NAT (Network Address Translation) と呼ばれるアドレス変換手法が両空間の境界で必要になる。NAT は、社内のみで通用するプライベート IP アドレスと、インターネット (外部) アクセスに利用できる本来のグローバルな IP アドレスを相互に変換する。これによって、ローカルな IP アドレスしか割り当てられていないノードであっても、透過的にインターネットにアクセスすることが可能となる。

【0007】

上述のような IP アドレス変換に係る技術は、例えば、特許文献 1 に開示されている。

【0008】

(3) プライベート IP アドレス空間とグローバル IP アドレス空間にまたがる通信

次に、上述したプライベート IP アドレス空間からグローバル IP アドレス空間にまたがる通信の一例について説明する。図 2 は、プロキシ (Proxy) サーバを用いて、プライベート IP アドレス網からグローバル IP アドレス網へ通信する例を示す処理シーケンスである。

【0009】

プロキシサーバは、図 2 に示されるように、社内 (企業 A) のネットワークと外部 (The Internet) の間に置かれて、データの出入りを監視するソフトウェア装置である。プロキシサーバは、データの出入りを監視するために、内部からのデータフローをアプリケーションレイヤレベルで終端し、データを精査した上で、外部への転送を行うように機能するアプリケーションレイヤにおける中継装置

として機能する。

【 0 0 1 0 】

プライベート I P アドレス空間とグローバル I P アドレス空間にまたがる通信において、プロキシサーバを設置する目的には下記に示す 3 つがある。

【 0 0 1 1 】

(1) プロキシサーバを設置することにより、アプリケーションデータ内にある通信先（問合せ先）のホスト名をプロキシサーバが検出し、社内からの通信に適切か否かを判断する。不適切な通信であると判断された場合には、中継しないようにする。

【 0 0 1 2 】

即ち、プライベート I P アドレス網とグローバル I P アドレス網にまたがる通信は全てアプリケーションレイヤでの終端が必要であり、DMZ (DeMilitarized Zone) 上にあるプロキシサーバ (図 2 でいう Proxy.flab.fujitsu.com) 上で特定のアプリケーション (一般的には HTTP) のみをアプリケーションレイヤで中継することができる。また、プロキシサーバでは、一般的に、問合せ先 (通信先) の名前 (HTTP の場合は URL (Uniform Resource Locator) 中の FQDN (Fully Qualified Domain Name : 図 2 でいう A.outside.com)) により、通信の可否を決定することができる。

【 0 0 1 3 】

(2) プライベート I P アドレス網内に存在するグローバル I P アドレスを送信元アドレス (SRC address) または送信先アドレス (DST address) とするパケットを流通させない。

【 0 0 1 4 】

即ち、プライベート I P アドレス網とグローバル I P アドレス網にまたがる通信では、グローバル I P アドレス網への経路制御がプライベート I P 網で必要になるため、プライベート I P 網内の経路制御が複雑になる。しかし、プロキシサーバを設けることにより、名前解決において、プライベート I P アドレス網からグローバル I P アドレス網のアドレスを取得できないようにして、グローバル I P アドレスの経路情報をプライベートアドレス網内に流さないようにすることが

できる。

【0015】

(3) グローバルIPアドレス網上の端末からプライベートIPアドレス網への通信の禁止

グローバルIPアドレス網上の端末からプライベートIPアドレス網への通信を禁止することは、プライベートIPアドレス網とグローバルIPアドレス網間で通信を行うときに一般に留意すべき点として知られている。

【0016】

従来は、DNSのドメイン・ツリー構成により、グローバルIPアドレス網上からプライベートIPアドレス網内にある端末の名前解決を実施しないようにする、または、DMZ上に存在するアドレス変換装置によりグローバルIPアドレス網上にある端末を問合せ元（通信元）とするパケットを破棄するなどして、グローバルIPアドレス網上の端末からプライベートIPアドレス網への通信を禁止していた。

【0017】

その他、IPアドレス変換に係る技術としては、特許文献2に開示された技術がある。

【0018】

【特許文献1】

特開2000-156710号公報

【特許文献2】

特開2001-156852号公報

【0019】

【発明が解決しようとする課題】

しかしながら、上記のような現状のアドレス空間をまたがる通信方式では下記に示すような問題があった。

【0020】

(1) プロキシサーバの負荷

プロキシサーバは、プライベートIP網内外にまたがる各々のデータフローが

流れている期間中、常に代表でアプリケーション中継をする必要があり負荷が大きくなる。

【 0 0 2 1 】

(2) アプリケーションの限定

プロキシサーバはアプリケーション中継を行うため、アプリケーションがプライベート I P 網内外にまたがる通信のサポート対象外（例えば、I P 電話）となる場合には、プロキシサーバによって中継できるアプリケーションが限定されてしまう。また、特定のアプリケーションに対してプライベート I P 網外への通信を不許可にしたい場合には、ネットワーク管理者等がプロキシサーバを操作することによりアプリケーションが意図的に限定できてしまう。

【 0 0 2 2 】

本発明は上述のような問題を解決し、プロキシサーバを用いることなく（従来プロキシサーバが担っていた機能や役割を満たして）、プライベート I P アドレス網とグローバル I P アドレス網の境界上にある D N S サーバとアドレス変換装置の連携により、プライベート I P アドレス空間とグローバル I P アドレス空間にまたがる通信を実現することができる装置や方法を提供することを目的とする。

【 0 0 2 3 】

【課題を解決するための手段】

上記問題を解決するため、本発明は以下のような構成をとる。即ち、本発明の第一の態様は、名前／アドレス変換装置であって、通信元から送信される、通信先の名前に対応するアドレスの問合せを受信した場合に、通信元及び通信先がそれぞれ属するネットワーク種別に基づいて、通信元と通信先との間の通信の可否を判定する判定手段と、上記判定手段の判定結果に基づいて、上記名前に対応する通信先のアドレスを通信元に回答するか否かを判定する第 2 判定手段と、上記第 2 判定手段が通信先のアドレスを回答すると判定した場合に、通信先のアドレスを取得して通信元に回答する回答手段とを含む。

【 0 0 2 4 】

本発明の第一の態様によると、名前／アドレス変換装置が、通信元から通信先

の名前に対応するアドレスの問合せを受けると、判定手段は、通信元及び通信先がそれぞれ属するネットワーク種別に基づいて、通信元－通信先間の通信の可否を判定する。この判定結果に基づいて、第2判定手段は、上記問合せに含まれる名前に対応する通信先のアドレスを通信元に回答するか否かを判定する。通信先のアドレスを回答すると判定された場合には、回答手段は、通信先のアドレスを取得して通信元に回答する。このように第一の態様によれば、通信元と通信先との双方の条件に基づいて名前に対応するアドレスを回答するか否かを判定することができる。

【0025】

また、本発明の第二の態様は、名前／アドレス変換装置であって、第1ネットワーク及び第2ネットワークから送信される、通信先の名前に対応する通信先のアドレスの問合せを受信する受信手段と、上記問合せを送信した通信元、及び上記通信先がそれぞれ属するネットワークを識別する識別手段と、上記通信元が上記第1ネットワークに属し且つ上記通信先が上記第2ネットワークに属する場合には、上記通信元に対して回答すべき上記通信先のアドレスを検索する検索手段と、上記通信先のアドレスを含む回答を送出する送出手段とを含み、上記送出手段は、上記通信元が上記第2ネットワークに属し且つ上記通信先が上記第1ネットワークに属する場合には、上記通信先のアドレスを含む回答を送出しない名前／アドレス変換装置である。

【0026】

本発明の第二の態様によると、名前／アドレス変換装置は、第1ネットワークから第2ネットワークに対して、通信先の名前に対応する通信先のアドレスの問合せが送信されると、受信手段は、上記問合せを受信する。識別手段は、受信した問合せから通信元及び通信先がそれぞれ属するネットワークを識別する。検索手段は、通信元が第1ネットワークに属し且つ通信先が第2ネットワークに属する場合には、問合せの送信元に対して回答するための通信先のアドレスを検索する。送出手段は、上記通信先のアドレスを含む回答を送出する。また、送出手段は、通信元が第2ネットワークに属し且つ通信先が第1ネットワークに属する場合には、通信先のアドレスを含む回答を送出しない。このように第二の態様によ

れば、通信元と通信先とが属するネットワーク種別を識別し、そのネットワーク種別に応じて通信先のアドレスを回答するか否かを決定することができる。即ち、第1ネットワークからは第2ネットワーク側への名前解決が行え、第2ネットワークからは第1ネットワーク側への名前解決が行えないようにすることができる。第1ネットワークの安全性を高めることができる。例えば、第1ネットワークには、プライベートIPアドレス網を適用し、第2ネットワークには、グローバルIPアドレス網を適用することができる。

【0027】

好ましくは、第二の態様における送出手段は、上記第1ネットワークに属する通信元と上記第2ネットワークに属する通信先との間での通信で使用が許可されたアプリケーションがない場合には、上記通信元へ上記通信先のアドレスを回答しないように構成することができる。

【0028】

この場合、送出手段は、通信元と通信先間の通信で使用が許可されたアプリケーションがない場合には、通信元に対して通信先のアドレスを回答しない。これによって、第1ネットワークと第2ネットワーク間で使用が許可されていないアプリケーションの使用による通信を防止できる。

【0029】

好ましくは、第2の態様における名前／アドレス変換装置は、上記第1ネットワークに属する通信元に相当する第1端末に対して上記第2ネットワークに属する通信先に相当する第2端末のアドレスが回答される場合に、上記第1ネットワークと上記第2ネットワークとの間を転送されるデータを受信して通過が許可されたデータのみを通過させるとともに上記第1ネットワークと上記第2ネットワークとの間のアドレス変換を行う中継装置に対し、上記第1端末と上記第2端末との間を転送されるデータを通過させるための通過情報を通知する通知手段をさらに含んでもよい。

【0030】

この場合、名前／アドレス変換装置から、第2端末のアドレスが回答される場合には、通知手段は、中継装置に対して、第1-第2端末間で転送されるデータ

を通過させるための通過情報を通知する。これによって、第1ネットワークと第2ネットワーク間で転送されるデータに対し、名前／アドレス変換装置で名前解決を行った端末間のデータを通過させるように中継装置を制御することができ、中継装置において、通過が許可されていないデータを排除（遮断）することができる。

【0031】

好ましくは、第二の態様における通知手段は、上記中継装置が上記第2端末から送信されるデータを通過させるときに、このデータに送信元アドレスとして付加された上記第2端末の上記第2ネットワークにおけるアドレスを上記第1ネットワークのアドレスに変換するために、上記第2端末に対して仮想的に割り当てられる上記第1ネットワークのアドレスと上記第2端末の上記第2ネットワークにおけるアドレスとを含む通過情報とを上記中継装置に通知し、上記送出手段は、上記第1端末が上記第2端末宛のデータに上記第2端末の上記第1ネットワークにおけるアドレスを送信先アドレスとして付加して送信し、且つ上記中継装置が上記第2端末宛のデータを通過させるときにこのデータに付加された送信先アドレスを上記第2端末の上記第2ネットワークにおけるアドレスに変換するために、上記第2端末の上記第1ネットワークにおけるアドレスを含む回答を送出するように構成することができる。

【0032】

この場合、通知手段は、第2端末に仮想的に割り当てられる第1ネットワークのアドレスと第2ネットワークにおけるアドレスとを中継装置に通知する。送出手段は、第1端末からの問合せに対し、第2端末の第1ネットワークにおけるアドレスを含む回答を送出する。これによって、第2ネットワークのアドレスが第1ネットワークに紛れ込むことを防止でき、また第1端末は第2端末を第1ネットワーク内の端末として認識することができる。従って、第2ネットワークの端末に仮想的に割り当てた第1ネットワーク内で使用できるアドレスを用いて、第1ネットワーク内で第2ネットワークの経路制御を行うことなく、異なる両アドレス空間の通信を実現することができ、且つ、第1ネットワークと第2ネットワークの経路の独立性を保障することができる。

【0033】

好ましくは、第二の態様における通知手段は、上記中継装置が上記第1端末と上記第2端末との間での利用が許可されたアプリケーションに基づくデータのみを通過させるために、上記第1端末と上記第2端末との間の通信での利用が許可されたアプリケーションに係る情報をさらに含む通過情報を上記中継装置に通知するように構成することができる。

【0034】

このような場合では、中継装置は、第1端末と第2端末間の通信において、利用が許可されたアプリケーションに係るデータのみを通過させる。これによって、第1-第2端末間で利用が許可されていないアプリケーションを用いた通信を防止できる。

【0035】

好ましくは、第2の態様における通知手段は、上記送出手段が上記第2端末のアドレスを送出する前に、上記通過情報を上記中継装置に通知するように構成することもできる。

【0036】

この場合、第2端末のアドレスを含む回答が到着する前に、既に中継装置に当該データを通過させるための通過情報（フィルタリング情報）が登録されているように構成することができる。これによって、名前／アドレス変換装置は中継装置と連携することにより、通信元が通信先へデータを送るための動作を効率的に矛盾なく実施できるようにすることができる。

【0037】

第2の態様において説明した送出手段及び通知手段に係る構成は、第1の態様に適用することもできる。

【0038】

また、本発明は、コンピュータが名前／アドレス変換装置として第1及び第2の態様に示した動作を行う方法として特定することもできる。また、本発明は、コンピュータが第1及び第2の態様における名前／アドレス変換装置として機能するためのプログラム、又はこのプログラムを記録した記録媒体として特定する

こともできる。

【0039】

本発明は、プライベートIPアドレス空間とグローバルIPアドレス空間にまたがる通信において、名前／アドレス変換装置が中継装置と連携するシステムに適用可能である。

【0040】

【発明の実施の形態】

《実施形態》

以下、図面を用いて本発明の実施形態について説明する。以降、本実施形態では、名前解決を要求する通信元となる端末を問合せ元とし、名前解決要求に対し通信先となる端末を問合せ先として説明し、パケットの問合せ元を示すアドレスを送信元アドレスとし、パケットの問合せ先を示すアドレスを送信先アドレスとして説明する。なお、本実施形態の説明は例示であり、本発明の構成は以下の説明に限定されない。

【0041】

〈概要〉

本実施形態に係るプライベートIPアドレス空間とグローバルIPアドレス空間にまたがる通信の概要を図3を用いて説明する。図3は、プライベートIPアドレス網からグローバルIPアドレス網への通信を示す図である。本実施形態では、プライベートIPアドレス空間とグローバルIPアドレス空間にまたがる通信において、従来プロキシサーバが担っていた機能を、プライベートIPアドレス網とグローバルIPアドレス網の境界上にあるDNSサーバ（図3におけるGlobal Cを持つDNSサーバ1）とアドレス変換装置とがそれぞれ役割分担する。即ち、DNSサーバ1は、名前（通信したい端末のホスト名またはドメイン名）により接続先のフィルタリングをする役割を担い、特定の条件に合致するデータのみに通過させるように機能する。アドレス変換装置は、問合せ先のポート番号によりアプリケーションをフィルタリングする役割を担い、アドレス変換機能とフィルタリング機能とを併せ持つアドレス変換・フィルタリング装置3として機能する。なお、アドレス変換・フィルタリング装置3は、プロキシサーバのような

アプリケーションレイヤでの終端機能を有さず、アドレス変換とそれに必要なセッション管理、及びフィルタリングを行うこととする。

【0042】

次に、本実施形態を実現するために生ずる要件についてそれぞれ説明する。

【0043】

(1) ネットワーク構成

ネットワーク構成として、従来のネットワーク構成に追加する要件を主に説明する。

【0044】

第一に、DNSは、その仕様上、問合せ元（通信元）端末が、問合せ先（通信先）端末がプライベートIPアドレス網上にあるか、グローバルIPアドレス網上にあるかを意識して、DNSサーバを使い分けることができない。このため、プライベートIPアドレス網上のDNSサーバ1とグローバルIPアドレス网上的DNSサーバ6とはドメイン・ツリー上で接続する。

【0045】

第二に、DNSサーバ1は、プライベートIPアドレス網における名前解決とグローバルIPアドレス網における名前解決との双方を扱う必要がある。このため、DNSサーバ1は、グローバルIPアドレス網側のドメイン・ツリーにも属する必要がある。従って、本発明の対象となるDNSサーバ1はグローバルIPアドレス網上(DMZ上)に配置される。

【0046】

第三に、プライベートIPアドレス網はグローバルIPアドレス網に対する経路を有していない。このため、プライベートIPアドレス網からはグローバルIPアドレス網全体が一つのプライベートIPアドレス網のサブネットとして見えるように構成する。即ち、図4に示すように、企業A側からみて、外部ネットワーク(The internet)が一つのサブネットに見えるように構成する。

【0047】

以下、上記のネットワーク構成を踏まえた装置別の要件を説明する。

【0048】

(2) DNSサーバ

次に、本発明の対象となるDNSサーバ1に対して必要となる要件について説明する。

【0049】

第一に、DNSサーバ1は、グローバルIPアドレス網内からの問合せであるか、またはプライベートIPアドレス網内からの問合せであるかを識別するための名前解決の問合せ元識別機能を有するように構成される。

【0050】

第二に、DNSサーバ1は、名前解決の問合せ元識別情報に基づいて、プライベートIPアドレス網内からの名前解決の問合せのみを対象とする名前解決要求に対する回答可否を判断する機能を有するように構成される。DNSサーバ1は、プライベートIPアドレス網上のDNSサーバ4と、グローバルIPアドレス網上のDNSサーバ6とが接続されている。このため、例えば、図5に示すように名前解決要求の問合せ元と問合せ先（解決する名前を持つ端末の位置）に応じた名前解決要求に対する回答を変更できるように構成される。

【0051】

名前解決要求の問合せ元と問合せ先に応じたDNSサーバの回答、及び動作について図5を用いて説明する。第一に、プライベートIPアドレス網からプライベートIPアドレス網内への端末装置（ホスト）への問合せ（名前解決要求）に対しては、通常のプライベートIPアドレス網上のDNSサーバとして動作する（図5の①に該当）。第二に、グローバルIPアドレス網からプライベートIPアドレス網内の端末装置への名前解決要求に対しては、名前解決要求を棄却する（図5の②に該当）。第三に、プライベートIPアドレス網からグローバルIPアドレス網内の端末装置への名前解決要求に対しては、接続可否を判断して回答する（図5の③に該当）。第四に、グローバルIPアドレス網からグローバルIPアドレス網内の端末装置への名前解決要求に対しては、通常のグローバルIPアドレス網上のDNSサーバとして動作する（図5の④に該当）。

【0052】

なお、③の動作を行うため、DNSサーバ1は、接続を許可するグローバルI

Pアドレス網上の名前毎に許可するポート番号も名前解決に必要な情報と共に管理する。この場合、DNSサーバ1は接続先のIPアドレスと共に対応するポート番号をアドレス変換・フィルタリング装置3に通知する。さらに、③の動作において、DNSサーバ1は、問合せ先となるグローバルIPアドレス網上の端末に仮想的に割り当てられたプライベートIPアドレスを名前解決の結果として返すように機能する。この仮想的なアドレスは、プライベートIPアドレス網の管理者によりDNSサーバ1に予め設定される。

【0053】

第三に、DNSサーバ1は、名前解決要求に対して回答をする場合、IPアドレス（プライベートIPアドレス）と、そのアドレス変換の対象となるIPアドレス（グローバルIPアドレス）、及びポート番号をアドレス変換・フィルタリング装置3へ通知するためのアドレス変換・フィルタリング装置3とのネゴシエーション機能を有するように構成される。

【0054】

（3）アドレス変換・フィルタリング装置

次に、アドレス変換・フィルタリング装置3に対して必要となる要件について説明する。アドレス変換・フィルタリング装置3は、DNSサーバ1からの通知に基づくパケットフィルタリング機能を提供する。即ち、アドレス変換・フィルタリング装置3は、プライベートIPアドレス側から受信するパケットに対して、転送先となるグローバルIPアドレス及びポート番号に基づいてフィルタリングを行い、受信したパケットを転送または廃棄する。また、アドレス変換・フィルタリング装置3は、NAT機能を有しており、仮想的に割り当てられたプライベートIPアドレスとグローバルIPアドレスへのアドレス変換を問合せ先毎に行う。

【0055】

〈ネットワーク構成〉

次に、本発明の実施形態を実現するためのネットワーク構成について図3を用いて説明する。

【0056】

図3に示す例では、プライベートIPアドレス網として、企業A内のネットワークに收容される端末（ホスト）2とDNSサーバ4とを含むネットワークが示されている。また、グローバルIPアドレス網として、インターネットが示されており、インターネットにサーバ（ホスト）5とDNSサーバ6とが接続されている。

【0057】

プライベートIPアドレス網とグローバルIPアドレス網との間には、ネットワーク上の中間地帯（DMZ）が存在する。ネットワーク上の中間地帯には、DNSサーバ1（本発明の対象となるDNSサーバ）、アドレス変換・フィルタリング装置3、L2-SW7、ルータ8がそれぞれ配置され、プライベートIPアドレス網側から、アドレス変換・フィルタリング装置3、L2-SW（レイヤスイッチ）7、ルータ8の順に接続され、DNSサーバ1（本発明の対象となるDNSサーバ）は、L2-SW7に接続されている。

【0058】

また、ネットワークを構成する各サーバや装置には、それぞれ異なるIPアドレス（プライベートIPアドレスやグローバルIPアドレス）が設定されている。図3に示す例では、ネットワークの中間地帯に位置するDNSサーバ1には、グローバルIPアドレス“Global C”とプライベートIPアドレス“Private D”とが設定されている。また、アドレス変換・フィルタリング装置3には、グローバルIPアドレス“Global A”とプライベートIPアドレス“Private C”とが設定されている。また、プライベートIPアドレス網内に位置するDNSサーバ4には、プライベートアドレス“Private B”が設定されている。また、グローバルIPアドレス網内に位置するDNSサーバ6には、グローバルIPアドレス“Global E”が設定されている。

【0059】

また、プライベートIPアドレス網内の端末2とグローバルIPアドレス網内に存在するサーバ5には、IPアドレスと特定のアプリケーションを利用する場合に使用されるポート番号とが割り当てられている。図3に示す例では、プライ

ベート IP アドレス網内に位置する端末 2 には、プライベート IP アドレス “P r i v a t e A” とポート番号 “P o r t X X” とが割り当てられている。また、グローバル IP アドレス網内に位置するサーバ 5 は、グローバル IP アドレス “G l o b a l D” と、仮想的に割り当てられたプライベート IP アドレス “P r i v a t e E” とポート番号 “P o r t Y Y” とが割り当てられている。また、サーバ 5 は、本実施形態において、問合せ先となり、名前（ホスト名またはドメイン名）として「A. o u t s i d e. c o m」を有している。

【0060】

なお、L 2 - S W 7 とルータ 8 は、プライベート IP アドレス網とグローバル IP アドレス網との間のトラフィックを中継する中継装置として機能する。また、L 2 - S W 7 は、ルータ 8 - アドレス変換・フィルタリング装置 3 間を転送されるパケットを DNS サーバ 1 へ転送する、或いは DNS サーバ 1 からのパケットをアドレス変換・フィルタリング装置 3 へ転送するための切替スイッチとして機能する。

【0061】

〈DNS サーバのシステム構成〉

次に、本発明の実施形態を実現するための DNS サーバ 1 のシステム構成について図 6 を用いて説明する。図 6 は、DNS サーバ 1 のシステム構成図を示す。

【0062】

DNS サーバ 1 は、通信終端部 10 と、受信識別部 11 と、送信パケット作成部 12 と、名前解決要求問合せ元識別部 13 と、名前解決要求問合せ先識別部 14 と、名前解決部 15 と、通信許可ポート検索部 16 と、アドレス割当部 17 と、アドレス返却部 18 と、アドレスプール管理部 19 と、名前解決回答作成部 20 と、アドレス変換・フィルタリング装置への通知作成部 21 とを備えている。DNS サーバ 1 は、パーソナルコンピュータやワークステーション等の情報処理装置を用いて構成され、その他の DNS サーバ 4, 6 と連携して問合せ先の名前（例えば、ホスト名またはドメイン名）から IP アドレスを取得して名前解決を図る。

【0063】

通信終端部 10 は、ネットワークからの通信を電氣的に終端する。ネットワークから受信した情報はパケットとして、受信識別部 11 へ渡される。また、送信パケット作成部 12 からのパケットは電氣的にネットワークへ送信する。

【0064】

受信識別部 11 は、パケット情報を識別する。受信識別部 11 は、送信されてきたパケットに対して、二つの役割を担うように機能する。第一に、受信識別部 11 は、正常パケットであるか異常パケット（例えば、フレーム形式が通常でない場合など）であるかを判断する。第二に、受信識別部 11 は、名前解決要求のパケット（名前解決要求パケット）であるかアドレス返却を通知するパケット（回答パケット）であるか、それ以外のパケットであるかを判断する。

【0065】

送信パケット作成部 12 は、ネットワーク上に送信するための情報をパケット化し、通信終端部 10 へ渡す。

【0066】

名前解決要求問合せ元識別部 13 は、名前解決要求の問合せ元端末がグローバル IP アドレス網上にあるか、またはプライベート IP アドレス網上にあるかを名前解決要求パケットの送信元 IP アドレスの種別に基づいて判断する。

【0067】

名前解決要求問合せ先識別部 14 は、名前解決をする問合せ先端末がグローバル IP アドレス網上にあるか、またはプライベート IP アドレス網上にあるかを問合せ先の名前に基づいて判断する。例えば、図 6 では、ドメイン名 “fujitsu.com” が名前解決の問合せ先に含まれている場合にはプライベート IP アドレス網内の端末に対する名前の解決要求であると判断し、それ以外の場合にはグローバル IP アドレス網内の端末に対する名前の解決要求であると判断する。なお、ここでの判定条件（fujitsu.com）は予め指定される。

【0068】

名前解決部 15 は、名前解決要求問合せ元識別部 13 と名前解決要求問合せ先識別部 14 との判断結果に基づいて受信した名前解決要求が図 5 に示す①, ②, ③, ④の何れに属するかを判断し、各々に対応する処理を実行する。即ち、名前解

決部 15 は、名前解決要求が①に属すると判断する場合には、自身が管理する名前・アドレスデータベース 15 a（プライベート）を検索する。また、名前解決部 15 は、名前解決要求が②に属すると判断する場合には、名前解決要求を棄却する。また、名前解決部 15 は、名前解決要求が③または④に属すると判断する場合には、自身が管理する名前・アドレスデータベース（グローバル） 15 b を検索する。なお、ここでの判断条件（例えば、図 5）は予め設定される。

【0069】

各名前・アドレスデータベース 15 a、15 b は、名前解決部 15 と接続されている。名前・アドレスデータベース 15 a、15 b は、それぞれ、問合せ先の名前とその回答である IP アドレスとの対応を保持するテーブル 15 a-1、15 b-1 を有する。

【0070】

通信許可ポート検索部 16 は、名前解決要求が図 5 に示す③に属する場合に、接続が許可されているポートを自身が管理する通信許可ポートリスト 16 a から検索する。

【0071】

通信許可ポートリスト 16 a は、通信許可ポート検索部 16 に接続されており、問合せ先の名前とその問合せ先への通信を許可するポート番号（アプリケーション）の一覧を示すテーブル 16 a-1 を有しているデータベースである。通信許可ポートリスト 16 a は、問合せ先の名前から、その名前に対して許可されているポート番号を検索して通信許可ポート検索部 16 に検索結果として返す。また、検索結果が未ヒットの場合には、通信不許可とする。なお、通信許可ポートリスト 16 a の内容は、予め設定される。

【0072】

アドレス割当部 17 は、名前解決要求が図 5 に示す③に属する場合に、プライベート IP 網側に通知する名前解決要求に対する仮のアドレス（仮想のプライベート IP アドレス）をアドレスプール管理部 19 を介してアドレスプールリスト 19 a から検索する。

【0073】

アドレス返却部 18 は、アドレス変換・フィルタリング装置 3 から返却された IP アドレス（プライベート IP アドレス）をアドレスプール管理部 19 を介してアドレスプールリスト 19 a に書込む。

【0074】

アドレスプール管理部 19 は、アドレスプールリスト 19 a を管理しており、アドレス割当部 17 またはアドレス返却部 18 と連携して、アドレスプールリスト 19 a に対するアドレス検索処理やアドレス登録処理を実行する。

【0075】

アドレスプールリスト 19 a は、プライベート IP 網側に通知する名前解決要求に対する仮のアドレス（仮想のプライベート IP アドレス）とその割当状態と対応関係の一覧を示すテーブル 19 a-1 を有するデータベースである。割当状態は、「割当中」または「未割当」により示される。また、割当状態が「割当中」である場合には、その割当先の名前も対応させて保持する。

【0076】

名前解決回答作成部 20 は、名前解決要求の問合せ元への回答を作成する。この場合、名前解決部 15 において検索に成功した場合には、解決した IP アドレスを内容とする回答を作成する。また、名前解決部 15 において検索に失敗した場合には、名前解決の失敗を内容とする回答を作成する。

【0077】

アドレス変換・フィルタリング装置への通知作成部 21 は、名前解決要求が図 5 に示す③に属する場合に、アドレス変換・フィルタリング装置 3 への通知内容を作成する。通知内容は、第一に、通信許可ポート検索部 16 で得たポート番号であり、第二に、アドレス割当部 17 で得たプライベート IP アドレスであり、第三に、名前解決部 15 で得たグローバル IP アドレスであり、第四に、問合せ先の名前である。

【0078】

〈アドレス変換・フィルタリング装置のシステム構成〉

次に、本発明の実施形態を実現するためのアドレス変換・フィルタリング装置 3 のシステム構成について図 7 を用いて説明する。図 7 は、アドレス変換・フィ

ルタリング装置 3 のシステム構成図を示す。

【 0 0 7 9 】

アドレス変換・フィルタリング装置 3 は、通信終端部 3 1 と、受信識別部 3 2 と、送信パケット作成部 3 3 と、フィルタ書換え部 3 4 と、アドレス書換え・フィルタ部 3 6 と、タイマ部 3 7 と、設定完了通知部 3 8 と、N A T 部 3 9 と、返却通知作成部 4 0 と、アドレス書換え・フィルタデータベース 3 5 とを備えている。アドレス変換・フィルタリング装置 3 は、通信機能を持つパーソナルコンピュータやワークステーション等の情報処理装置を用いて構成され、N A T (NAPT : Network Address Port Translation) によるアドレス変換機能と、受信するパケット毎の I P アドレス及びポート番号に基づいてそのパケットをフィルタリングする機能とを併せ持つ。

【 0 0 8 0 】

通信終端部 3 1 は、ネットワークからの通信を電氣的に終端する。ネットワークから受信した情報はパケットとして、受信識別部 3 2 へ渡す。また、送信パケット作成部 3 3 からのパケットは電氣的にネットワークへ送信する。

【 0 0 8 1 】

受信識別部 3 2 は、パケット情報の識別を行う。受信識別部 3 2 では、送信されてきたパケットに対して、二つの役割を担うように機能する。第一に、受信識別部 3 2 は、正常パケットであるか異常パケット（例えば、フレーム形式が通常でない場合など）であるかを判断する。第二に、受信識別部 3 2 は、D N S サーバ 1 からの通知パケットであるか、それ以外のデータパケットであるかを判断する。

【 0 0 8 2 】

送信パケット作成部 3 3 は、ネットワーク上に送信するための情報をパケット化し、通信終端部 3 1 へ渡す。

【 0 0 8 3 】

フィルタ書換え部 3 4 は、受信した通知パケットに基づいて、アドレス書換え・フィルタデータベース 3 5 a を書換える。書換える内容は、第一に、D N S サーバ 1 の通信許可ポート検索部 1 6 で取得され、アドレス変換・フィルタリング

装置 3 に通知されたプライベート IP アドレスであり、第二に、DNS サーバ 1 の名前解決部 15 で取得され、アドレス変換・フィルタリング装置 3 に通知されたグローバル IP アドレスであり、第三に、DNS サーバ 1 の通信許可ポート検索部 16 で取得され、アドレス変換・フィルタリング装置 3 に通知されたポート番号である。

【0084】

アドレス書換え・フィルタデータベース 35 は、DNS サーバ 1 からの通知パケットに基づいて作成される。データベース 35 は、プライベート IP アドレスとグローバル IP アドレスと、通信許可ポート番号と、最終アクセス時刻との対応を一つのエントリとした一覧を保持するテーブル 35a を有する。また、アドレス書換え・フィルタデータベース 35 は、フィルタ書換え部 34 と、アドレス書換え・フィルタ部 36 と、タイマ部 37 とに接続されており、それぞれ連携して機能する。

【0085】

アドレス書換え・フィルタ部 36 は、データパケット毎にデータを書換える。第一に、アドレス書換え・フィルタ部 36 は、プライベート IP アドレス網からグローバル IP アドレス網へのパケットに対しては、まず、パケットの送信先 IP アドレス（プライベート IP アドレス）に基づいてアドレス書換え・フィルタデータベース 35 を検索し、対応するグローバル IP アドレスをパケットの送信先 IP アドレスとして書き換える。同時に、パケットの送信先ポート番号が検索結果のポート番号と一致しているか否かを確認する。一致している場合には、グローバル IP アドレス網へパケットを送信し、一致していない場合には、パケットを破棄する。また、アドレス書換え・フィルタ部 36 は、アドレス書換え・フィルタデータベース 35 における最終アクセス時刻を更新する。第二に、アドレス書換え・フィルタ部 36 は、グローバル IP アドレス網からプライベート IP アドレス網へのパケットに対しては、まず、パケットの送信元 IP アドレス（グローバル IP アドレス）に基づいてアドレス書換え・フィルタデータベース 35 を検索し、対応するプライベート IP アドレス（仮想のアドレス）をパケットの送信元 IP アドレスとして書換える。また、パケットの送信元ポート番号が検索

結果のポート番号と一致しているか否かを確認する。一致している場合には、プライベートIPアドレス網へパケットを送信し、一致していない場合には、パケットを破棄する。また、アドレス書換え・フィルタ部36は、アドレス書換え・フィルタデータベース35における最終アクセス時刻を更新する。

【0086】

タイマ部37は、アドレス書換え・フィルタデータベース35の各エントリにおける最終アクセス時刻を定期的に確認し、一定時間アクセスされていないエントリがある場合には、該エントリを削除する。

【0087】

設定完了通知部38は、DNSサーバ1から受信した通知パケットに基づいてアドレス書換え・フィルタデータベース35の書換えが終了したことをDNSサーバ1に通知する情報（通知情報）を作成する。通知情報は、フィルタ書換えの終了通知と、通信許可ポート検索部16で得たポート番号と、アドレス割当部17で得たプライベートIPアドレスと、名前解決部15で得たグローバルIPアドレスと、問合せ先の名前とを含む。

【0088】

NAT部39は、NAT（NAPT）処理（RFC3022に規定）を行う。即ち、NAT部39は、グローバルIPアドレスとプライベートIPアドレス間の変換処理を行う。

【0089】

返却通知作成部40は、タイマ部37によりタイムアウトが検出されたアドレス書換え・フィルタデータベース35の最終アクセス時刻を含むエントリを除く、他のエントリ（有効なエントリ）の情報をDNSサーバ1に通知する。

【0090】

〈パケットのデータ構造〉

次に、本実施形態において送受信されるパケットのデータ構造について図8を用いて説明する。

【0091】

図8は、プライベートIPアドレス空間とグローバルIPアドレス空間で送受

信されるパケットのフォーマットを示す図である。

【0092】

図8に示されるように、パケット100は、送信先IPアドレスと送信元IPアドレスと送信先ポート番号と送信元ポート番号とを示すフィールドとその他の制御情報等を示すフィールドとを含んでいる。なお、パケット100については、本実施形態で関連する、送信先IPアドレスと送信元IPアドレスと送信先ポート番号と送信元ポート番号のみを取り上げて説明する。

【0093】

プライベートIPアドレス網からグローバルIPアドレス網へ送信されるパケットは、アドレス変換・フィルタリング装置3を通過する際に、アドレス書換え・フィルタ部36により送信先IPアドレスを示すフィールドが書換えられる。また、アドレス変換・フィルタリング装置3内のNAT部39では、通常のNAT(NAPT)処理により送信元IPアドレスと送信元ポート番号とを示すフィールドが書換えられる。

【0094】

グローバルIPアドレス網からプライベートIPアドレス網へ送信されるパケットは、アドレス変換・フィルタリング装置3を通過する際に、アドレス書換え・フィルタ部36により送信元IPアドレスを示すフィールドが書換えられる。また、アドレス変換・フィルタリング装置3内のNAT部39では、通常のNAT(NAPT)処理により送信先IPアドレスと送信先ポート番号とを示すフィールドが書換えられる。

【0095】

〈動作フロー〉

以下、本実施形態を実現する具体的な動作について図3、図9～図15を用いて各パターン毎に説明する。

【0096】

〔プライベートIPアドレス網内からグローバルIPアドレス網への通信〕

(1) 通信許可時

図3は、通信許可時におけるプライベートIPアドレス網からグローバルIP

アドレス網への通信を示す処理シーケンスである。以下、図面上において、ネットワーク網間において送受信されるパケットの内容は、D N S のフロー時（名前解決要求に係る通信）には「送信元アドレス（SRC address）／送信先アドレス（DST address）／問合せまたは回答（Query or Responce）」として表す。また、データフロー時（実際のアクセス開始に係る通信）には、「送信元アドレス（SRC address）／送信先アドレス（DST address）／送信元ポート番号（SRC Port）／送信先ポート番号（DST port）」として表す。なお、図面上において、D N S のフロー時のパケットを実線で表し、データフロー時のパケットは点線で表す。

【 0 0 9 7 】

図 3 において、プライベート I P アドレス網（企業 A 内のネットワーク）に收容されている端末 2 からグローバル I P アドレス網（The Internet）に收容されているサーバ 5 に対するパケットは、端末 2 とサーバ 5 との間に設置されているアドレス変換・フィルタリング装置 3，L 2 - S W 7，ルータ 8 を介して I P 網間を転送される。各 D N S サーバ 1，4，6 は、端末 2 及びサーバ 5 が通信先の I P アドレスを知るために利用される。そして、アドレス変換・フィルタリング装置 3 は、I P 網間を転送されるパケットのアドレス変換及びフィルタリングを司る。ここで、プライベート I P アドレス網（企業 A 内のネットワーク）とグローバル I P アドレス網（The Internet）の間に位置するネットワーク上の中間地帯（DMZ）が、アドレス変換・フィルタリング装置 3 - ルータ 8 間（以下、グレイゾーンと呼ぶ）であると仮定して説明する。なお、端末 2 とサーバ 5 間において通信する際、L 2 - S W 7 とルータ 8 を経由するが、それらの動作については説明を省略する。

【 0 0 9 8 】

まず、プライベート I P アドレス網（企業 A 内のネットワーク）に收容されている端末 2 からサーバ 5 へパケットを転送する場合には、端末 2 は、サーバ 5 の I P アドレスを知るために、同一ネットワーク内に存在する D N S サーバ 4 宛に名前解決要求パケットを送信する（S 1）。この場合、送信されるパケットは「P r i v a t e A（端末 2 のプライベート I P アドレス：送信元アドレス）」

、「Private B (DNSサーバ4のプライベートIPアドレス:送信先アドレス)」,及び「A.outside.com (問合せ:名前解決対象のホスト(サーバ5)の名前)」を含む。

【0099】

次に、DNSサーバ4は、自身が持つゾーンの情報では名前解決を行うことができないので、グレイゾーン上に位置するDNSサーバ1を送信先アドレスに設定した名前解決要求パケットを送信する(S2)。この時の名前解決要求パケットは「Private B (DNSサーバ4のプライベートIPアドレス:送信元アドレス)」,「Private D (DNSサーバ1のプライベートIPアドレス:送信先アドレス)」,及び「A.outside.com (問合せ:サーバ5のホスト名)」を含む。グレイゾーン上において、DNSサーバ4から送信された名前解決要求パケットは、アドレス変換・フィルタリング装置3を経由する。アドレス変換・フィルタリング装置3は、名前解決要求パケットの送信元IPアドレスと送信先IPアドレスとをプライベートIPアドレスからグローバルIPアドレスに変換したパケットを送信する(S3)。これによって、アドレス変換・フィルタリング装置3を通過した後の名前解決要求パケットは、「Global A (アドレス変換・フィルタリング装置3のグローバルIPアドレス:送信元アドレス)」,「Global C (DNSサーバ1のグローバルIPアドレス:送信先アドレス)」,及び「A.outside.com」を含む。

【0100】

続いて、グレイゾーン上に位置するDNSサーバ1は、自身が持つゾーンの情報では名前解決を行うことができないので、グローバルIPアドレス網に收容されているDNSサーバ6宛に名前解決要求パケットを送信する(S4)。この名前解決要求パケットは、「Global C (DNSサーバ1のグローバルIPアドレス:送信先アドレス)」,「Global E (DNSサーバ6のグローバルIPアドレス:送信先アドレス)」,及び「A.outside.com」を含む。

【0101】

DNSサーバ6は、DNSサーバ1から受信した名前解決要求パケットに基づ

いて名前解決を行い、その結果、サーバ5のグローバルIPアドレス(Global D)を得る。そして、DNSサーバ6は、名前解決の結果を含むパケット(回答パケット)をDNSサーバ1宛に送信する(S5)。即ち、名前解決要求パケットの問合せ(A.outside.com)に対応するIPアドレスを含む回答パケットを送信する。回答パケットは、「Global E(送信元アドレス)」,「Global C(送信先アドレス)」,及び「Global D(回答:名前に対応するグローバルIPアドレス)」を含む。

【0102】

DNSサーバ1は、DNSサーバ6から回答パケットを受信する。すると、DNSサーバ1は、サーバ5の名前(ホスト名)に対して許可されているポート番号(アプリケーション識別子)を求めることで、通信を許可するか否かを判断する。ここでは、ポート番号「Port YY」が検索され、通信を許可すると判断したと仮定する。通信を許可する場合には、DNSサーバ1は、サーバ5に割り当てる仮想のプライベートIPアドレス「Private E」を取得し、この「Private E」と、「Global D」と、「Port YY(通信許可ポート番号)」を含む通知パケット(登録依頼)をアドレス変換・フィルタリング装置3へ送信する(S6)。

【0103】

アドレス変換・フィルタリング装置3は、DNSサーバ1からの通知パケットの内容をデータベース35に登録する。登録が完了すると、登録完了を通知するパケットをDNSサーバ1に返す(S7)。

【0104】

DNSサーバ1は、登録完了の通知を受け取ると、DNSサーバ4への回答パケットを作成し、アドレス変換・フィルタリング装置3宛に送信する(S8)。回答パケットは、「Global C(送信元アドレス)」,「Global A(送信先アドレス)」,及び「Private E(回答:名前に対応する仮想のプライベートIPアドレス)」を含む。この時、DNSサーバ1は、回答として、サーバ5のグローバルIPアドレスを仮想のプライベートIPアドレスに変換する。これによって、回答パケットは、その宛先において、プライベートI

P 網中のホストから送信されたと認識することができる。

【0105】

アドレス変換・フィルタリング装置 3 は、DNS サーバ 1 から受信した回答パケットの送信元アドレスと送信先アドレスをグローバル IP アドレスからプライベート IP アドレスにアドレス変換し、DNS サーバ 4 宛に送信する (S9)。この時、回答パケットは「Private D (送信元アドレス)」, 「Private B (送信先アドレス)」, 及び「Private E」を含む。

【0106】

DNS サーバ 4 は、回答パケットを受信すると、端末 2 に対し、名前解決要求に対する回答パケットを送信する (S10)。この時、回答パケットは「Private B (送信元アドレス)」, 「Private A (送信先アドレス)」, 及び「Private E」を含む。

【0107】

名前解決要求パケットを送信した端末 2 は、DNS サーバ 4 から受信した回答パケットの内容から問合せに対する回答が「Private E」であることを知る。即ち、端末 2 は、問合せた名前 (A.outside.com) に対応する IP アドレスが「Private E」であることを知る。

【0108】

端末 2 は、サーバ 5 と通信を開始するために、データパケットを送信する (S11)。この場合、データパケットのヘッダには「Private A (送信元アドレス)」, 「Private E (送信先アドレス)」, 「XX (送信元ポート番号)」, 及び「YY (送信先ポート番号)」が設定される。

【0109】

端末 2 から送信されたデータパケットは、グレイゾーン上でアドレス変換・フィルタリング装置 3 を通過する。この時、アドレス変換・フィルタリング装置 3 は、データパケットの送信先ポート番号に基づいて通信の可否を判断し、送信先ポート番号が通信が許可されているポート番号であれば、通過可能であると判断し、このデータパケットの送信先アドレスと送信元アドレスとをプライベート IP アドレスからグローバル IP アドレスにアドレス変換して通過させる。この時

アドレス変換・フィルタリング装置 3 から送出されるデータパケットのヘッダは「G o l b a l A (送信元アドレス)」, 「G l o b a l D (送信先アドレス)」, 「X X (送信元ポート番号)」, 及び「Y Y (送信先ポート番号)」を含む状態となる (S 1 2)。

【0110】

サーバ 5 は、端末 2 からのデータパケットを受け取るとそのパケットの送信元である問合せ元端末 2 に対し、データパケットを送信する (S 1 3)。この場合、データパケットのヘッダは「G o l b a l D (送信元アドレス)」, 「G l o b a l A (送信先アドレス)」, 「Y Y (送信元ポート番号)」, 及び「X X (送信先ポート番号)」となる (S 1 3)。

【0111】

サーバ 5 から送信されたデータパケットは、グレイゾーン上でアドレス変換・フィルタリング装置 3 を通過する。この時、データパケットの送信先アドレスと送信元アドレスは、グローバル IP アドレスからプライベート IP アドレスに変換される。これによって、アドレス変換・フィルタリング装置 3 から送出されるデータパケットのヘッダは「P r i v a t e E (送信元アドレス)」, 「P r i v a t e A (送信先アドレス)」, 「Y Y (送信元ポート番号)」, 及び「X X (送信先ポート番号)」を含む状態となる (S 1 4)。

【0112】

《A-A' 間、及び C 点における DNS サーバ 1 の動作フロー》

次に、図 3 において本実施形態を実現するための DNS サーバ 1 の動作について図 9 を用いて説明する。

【0113】

図 9 は、図 3 における DNS サーバ 1 の動作処理を示すフローチャートである。DNS サーバ 1 は、ネットワーク上からパケットを受信することを契機に動作する。通信終端部 10 は、ネットワーク上からのパケットを受信する (S 100)。

【0114】

受信識別部 11 は、名前解決要求パケットであるか否か、またはアドレス変換

・フィルタリング装置 3 内のアドレス書換え・フィルタ部 36 からのパケットであるか否かを識別する (S101)。

【0115】

この時、パケットフォーマットが異常である場合には、該パケットを破棄する (S102)。また、名前解決の要求・回答・アドレス返却、設定完了通知以外の正常パケットである場合には、当該パケットに応じたその他の処理を実行する (S103)。

【0116】

まず、DNSサーバ1の受信識別部11 (S101) において、パケットが名前解決の要求・回答であると識別された場合について説明する。S101において、パケットが名前解決の要求・回答であると識別された場合には、名前解決要求問合せ元識別部13は該パケットの送信元IPアドレスに基づいて問合せ元のネットワーク種別を識別する (S104)。続いて、パケットは名前解決要求問合せ先識別部14に渡され、問合せ先の名前に基づいて問合せ先のネットワーク種別を識別する (S105)。即ち、名前解決要求問合せ元識別部13及び名前解決要求問合せ先識別部14は、問合せ元または問合せ先がプライベートIPアドレス網であるのか、グローバルIPアドレス網であるのかを識別する。

【0117】

名前解決要求問合せ元識別部13と名前解決要求問合せ先識別部14とによる識別結果に基づいて、名前解決部15は、名前解決に利用するデータベースを決定する (S106)。即ち、図5に示すような、名前解決要求の問合せ元と問合せ先との組み合わせ条件に応じた処理を実施する。

【0118】

この時、問合せ元及び問合せ先が共にプライベートIPアドレス網又はグローバルIPアドレス網内に属する場合には、S116に処理が進み、図5の①の動作が行われる。一方、問い合わせ元がグローバルIPアドレス網内に属し、且つ問い合わせ先がプライベートIPアドレス網内に属する場合には、グローバルIPアドレス網からプライベートIPアドレス網への通信を禁止するため、名前解決要求を棄却する (図5の②)。

【0119】

S106において、パケットの問合せ先を示すIPアドレスがグローバルIPアドレス網内のアドレスである場合、即ち、図5の③、④に該当する場合には、名前解決部15は、名前・アドレスデータベース（グローバル）15bを検索する（S107）。この時、DNSサーバ1は、他のDNSサーバと連携し、他のDNSサーバで得られる変換先のIPアドレスを受け取ることによって、名前解決を行うこともできる。例えば、図3に示す例では、DNSサーバ1は、DNSサーバ6との連携により、変換先のIPアドレス「Global D」を得ている。

【0120】

S107において、名前解決部15が名前・アドレスデータベース（グローバル）15bを検索した結果、該当するIPアドレスがヒットした場合には通信許可ポート検索部16は、名前を検索キーとして、通信許可ポートリスト16aから通信を許可するポート番号を検索する（S108）。図3に示す例では、名前に対して許可されているアプリケーションのポート番号として、「Port Y Y」が得られている。なお、S108の検索結果、ヒットしなかった場合（以下、「ミスヒット」と表記する）には、名前解決失敗となりS112に進む。これは、許可されていないアプリケーションの通信を排除するためである。

【0121】

また、S107において、名前解決部15が名前・アドレスデータベース（グローバル）15bを検索した結果（連携の結果を含む）、ミスヒットであった場合には、問合せ元に対する回答は名前解決失敗となり、名前解決回答作成部20によりDNSサーバ1の回答を作成する（S112）。

【0122】

S108の検索結果において、名前に対応するポート番号がヒットした場合には、アドレス割当部17は、アドレスプール管理部19を介してアドレスプールリスト19aからプライベート網側に割り当てるプライベートIPアドレスを検索する（S109）。図3に示す例では、S109において、「Global D」に割り当てるべき仮想のプライベートIPアドレス「Private E」

がアドレスプールリスト 19 a から得られている。S 109 の検索結果がミスヒットであった場合には、名前解決失敗となり S 112 に進む。

【0123】

S 109 の検索結果において、該当するプライベート IP アドレスがヒットした場合には、アドレス通知作成部 21 がアドレス変換・フィルタリング装置 3 への通知パケット（登録依頼パケット）を作成する（S 110）。

【0124】

通知パケットは、通信先の IP アドレス(回答)、ポート番号、送信元 IP アドレス、送信先 IP アドレス、及び名前を含む。図 3 に示す例では、「P r i v a t e E」,「P o r t YY」,「G l o b a l D」,「P r i v a t e A」,及び「A. o u t s i d e. c o m」を含む通知パケットが作成されている。

【0125】

最終的に送信される通知パケットは、送信パケット作成部 12 に渡され、通信終端部 10 を経由して送信される（S 111）。

【0126】

以上は、図 3 に示す通信許可時のプライベート IP アドレス網からグローバル IP アドレス網への通信において、図 3 の A-A' 間における DNS サーバ 1 の動作である。DNS サーバ 1 は、A-A' 間では、「G l o b a l E」を持つ DNS サーバ 6 と連携して既存の DNS 処理を行う。即ち、図 9 に示されるように、DNS サーバ 1 は、A-A' 間において、S 100-S 101-S 104-S 105-S 106-S 107-S 108-S 109-S 110-S 111 の順に動作する。

【0127】

次に、DNS サーバ 1 の受信識別部 11（S 101）において、パケットが設定完了通知であると識別された場合について説明する。S 101 において、受信識別部 11 にてパケットが設定完了通知であると識別された場合には、名前解決回答作成部 20 が、問合せ元への回答としてアドレスプールリスト 19 a から取り出したプライベート IP アドレスを含む DNS の回答を作成する（S 112）

。図3に示す例では、問合せ元への回答となるプライベートIPアドレスとして「Private E」を含む回答パケットが生成される。

【0128】

最終的に、図3のS8において送信される回答パケットは、送信パケット作成部12に渡され、通信終端部10を経由して送信される（S111）。

【0129】

以上は、図3に示す通信許可時のプライベートIPアドレス網からグローバルIPアドレス網への通信において、図3のC点におけるDNSサーバ1の動作である。DNSサーバ1は、C点において、アドレス変換・フィルタリング装置3からの登録完了通知パケットの受信を契機に、S100-S101-S112-S111の順に動作する。

【0130】

《B点及びD点におけるアドレス変換・フィルタリング装置3の動作フロー》

次に、図3において本実施形態を実現するためのアドレス変換・フィルタリング装置3の動作について図10を用いて説明する。

【0131】

図10は、図3におけるアドレス変換・フィルタリング装置3の動作処理を示すフローチャートである。アドレス変換・フィルタリング装置3は、ネットワーク上からパケットを受信することを契機に動作する。通信終端部31は、ネットワーク上からのパケットを受信する（S120）。

【0132】

受信識別部32は、正常なパケットフォーマットから構成されるデータパケット（正常なパケットフォーマットであるか否かも確認する）であるか、または、DNSサーバ1からの通知パケット（登録依頼パケット）であるかを識別する（S121）。

【0133】

S121において、パケットフォーマットが異常であった場合には、該パケットを破棄する（S122）。S121において、パケットがデータパケットでもなく、通知パケットでもない場合には、当該パケットに応じたその他の処理が実

行される（S123）。

【0134】

まず、アドレス変換・フィルタリング装置3内の受信識別部32（S121）において、受信したパケットが通知パケットであると識別された場合について説明する。S121において、通知パケットであると識別された場合には、フィルタ書換え部34に通知され、通知パケット内に含まれるプライベートIPアドレスとグローバルIPアドレスと通信許可ポート番号とをアドレス書換え・フィルタデータベース35内に書込む（S124）。

【0135】

図3に示す例では、フィルタ書換え部34は、通知パケットに含まれた「Private E」,「Global D」,及び「Port YY」がデータベースに書込まれる。

【0136】

続いて、設定完了通知部38は、通知パケットに基づいてDNSサーバ1への設定完了通知を作成する（S125）。この場合、設定完了通知は、通信先のプライベートIPアドレス、通信先のグローバルIPアドレス、通信許可ポート番号、通信先の名前、及び書換え終了通知を含む。図3に示す例では、「Private E」,「Global D」,「Port YY」,「A. outside. com」,及び書換え終了通知を含む設定完了通知が生成される。

【0137】

続いて、送信パケット作成部33は、S125において作成した設定完了通知をパケット化して、通信終端部31から完了登録（図3のS7）としてDNSサーバ1に対して送信する（S126）。

【0138】

以上は、図3に示す通信許可時のプライベートIPアドレス網からグローバルIPアドレス網への通信において、図3のB点におけるアドレス変換・フィルタリング装置3の動作である。即ち、アドレス変換・フィルタリング装置3は、B点において、DNSサーバ1からの通知パケットの受信（S6）を契機に、S120-S121-S124-S125-S126の順に動作する。

【0139】

次に、アドレス変換・フィルタリング装置 3 内の受信識別部 3 2 (S 1 2 1) において、受信したパケットがデータパケットであると識別された場合について説明する。S 1 2 1 において、データパケットであると識別された場合には、アドレス書換え・フィルタ部 3 6 に通知され、アドレス書換え・フィルタ部 3 6 はアドレス書換え・フィルタデータベース 3 5 をデータパケットの送信先 IP アドレスをキーとして検索する (S 1 2 7)。

【0140】

この時、アドレス書換え・フィルタ部 3 6 は、送信元 IP アドレスに対応する IP アドレス(送信先 IP アドレスとしてのグローバル IP アドレスに対応するプライベート IP アドレス、または送信先 IP アドレスとしてのプライベート IP アドレスに対応するグローバル IP アドレス)がヒットした場合には、当該エントリに格納されているポート番号と、データパケットの送信先ポート番号とを対比し、両者が一致するか否かを判定する。そして、両者が一致する場合には、転送が許可されたデータパケットであると判定(ヒット)し、S 1 2 8 に処理を進める。これに対し、検索キーに対応する IP アドレスがない場合、または対応する IP アドレスが存在するがデータパケットの送信先ポート番号が通信許可されたポート番号に該当しない場合(ミスヒット)には、処理が S 1 3 0 に進む。

【0141】

S 1 2 7 の検索結果において、ヒットした場合には、データパケットのアドレスを書換える (S 1 2 8)。図 3 に示す例では、パケットの送信先 IP アドレスが「Private E」から「Global D」に書換えられている。続いて、NAT 部 3 9 において、一般的な NAT (NAPT) 処理が実行される (S 1 2 9)。送信パケット作成部 3 3 は、S 1 2 9 において NAT 処理が施されたデータをパケット化して、通信終端部 3 1 から送信する (S 1 2 6)。

【0142】

また、S 1 2 7 の検索結果において、ミスヒットであった場合には、該パケットが破棄される (S 1 3 0)。これによって、許可されていない IP アドレスへの通信や、許可されていないアプリケーションを利用した通信がフィルタリング

される。

【0143】

以上は、図3に示す通信許可時のプライベートIPアドレス網からグローバルIPアドレス網への通信において、図3のD点におけるアドレス変換・フィルタリング装置3の動作である。即ち、アドレス変換・フィルタリング装置3は、D点において、端末2からのデータパケットの受信(S11)を契機に、S120-S121-S127-S128-S129-S126の順に動作する。

【0144】

本発明によれば、プライベートIPアドレス空間とグローバルIPアドレス空間との境界上において、DNSサーバ1がアドレス変換・フィルタリング装置3と連携して両アドレス空間に必要とされる役割を分担して機能することにより、プライベートIPアドレス空間からグローバルIPアドレス空間にまたがる通信を可能にすることができる。

【0145】

(2) プライベートIPアドレスの返却

次に、プライベートIPアドレス網内からグローバルIPアドレス網内への通信(図5の③に該当)において、プライベートIPアドレスが返却される処理について図9、図10、図11を用いて説明する。

【0146】

図11は、プライベートIPアドレスの返却処理を示す処理シーケンスである。図11において、プライベートIPアドレスの返却は、データフローが一定時間流れず、アドレス変換・フィルタリング装置3のタイマ部37によりタイムアウトが検出された場合に、アドレス変換・フィルタリング装置3からDNSサーバ1に対して実行される。

【0147】

アドレス変換・フィルタリング装置3は、一定時間通信がない場合には、DNSサーバ1のアドレス割当部17で得たプライベートIPアドレスをDNSサーバ1に対して返却する(S21)。図3に示す例では、DNSサーバ1に対して「Private E」を返却される。

【0148】

《E点におけるアドレス変換・フィルタリング装置3の動作フロー》

次に、図11におけるE点の処理について、図10を用いて説明する。

【0149】

アドレス変換・フィルタリング装置3は、タイマ部37の監視結果を契機にプライベートIPアドレスの返却処理を実行する。アドレス変換・フィルタリング装置3内のタイマ部37は、定期的にアドレス書換え・フィルタデータベース35の各エントリの更新時刻を監視する(S131)。S131の監視、またはデータフローが一定時間流れなかった場合に、タイムアウトしたエントリを検出する(S132)。タイムアウトしたエントリを検出した場合には、該エントリのプライベートIPアドレスから、返却通知作成部40は、アドレスの返却通知を作成する(S133)。送信パケット作成部33は、S133において作成したアドレスの返却通知をパケット化して、通信終端部31からDNSサーバ1に対してプライベートIPアドレスの返却通知を送信する(S126)。図11に示す例では、「Private E」が返却されている。

【0150】

以上は、図11に示すプライベートIPアドレス網からグローバルIPアドレス網への通信において、図11のE点におけるアドレス変換・フィルタリング装置3の動作である。即ち、アドレス変換・フィルタリング装置3は、E点において、データフローが一定時間ない場合には、S131-S132-S133-S126の順に動作する。

【0151】

《F点におけるDNSサーバ1の動作フロー》

次に、図11におけるF点の処理について、図9を用いて説明する。

【0152】

DNSサーバ1は、ネットワーク上からパケットを受信することを契機に動作する。通信終端部10は、ネットワーク上からのパケットを受信する(S100)。

【0153】

受信識別部 11 は、名前解決要求パケットであるか否か、またはアドレス変換・フィルタリング装置 3 内のアドレス書換え・フィルタ部 36 からのパケットであるか否かを識別する (S101)。即ち、図 11 の F 点において、受信識別部 11 は、受信したパケットがアドレス変換・フィルタリング装置 3 からのアドレス返却時のパケットであることを識別する。

【0154】

受信識別部 11 (S101) において、パケットがアドレス返却であると識別されると、アドレス返却部 18 は、返却するプライベート IP アドレスを抽出する (S113)。続いて、アドレス返却部 18 は、アドレスプール管理部 19 を介してアドレスプールリスト 19a 内の該当するアドレスの状態を未割当に変更する (S114)。

【0155】

以上は、図 11 に示すプライベート IP アドレス網からグローバル IP アドレス網への通信において、図 11 の F 点における DNS サーバ 1 の動作である。即ち、DNS サーバ 1 は、F 点において、データフローが一定時間ない場合には、S100-S101-S113-S114 の順に動作する。

【0156】

本発明によれば、プライベート IP アドレス空間とグローバル IP アドレス空間にまたがる通信において、一定時間通信がない場合には、実施途中である名前解決要求を終了させ、名前解決を実施しないように機能することができる。即ち、一度 IP アドレスを割り当てた後に一定時間通信がない場合には、アドレスを返却することにより無駄に仮想アドレスを割り当てることを防ぐことができる。

【0157】

(3) 名前による通信拒否時

次に、名前による通信拒否時におけるプライベート IP アドレス網内からグローバル IP アドレス網内への通信 (図 5 の③に該当) について図 9、図 10、図 12 を用いて説明する。

【0158】

図 12 は、名前により通信を拒否する場合のプライベート IP アドレス網内か

らグローバル IP アドレス網内への通信を示す処理シーケンスである。ここでは、名前「A. outside. com」を持つサーバ 5 への通信を禁止する場合を想定して説明する。なお、図 1 2 は、図 3 の S 3 において名前解決が拒否された場合に実行される処理であり、S 3 1 と S 3 2 は、図 3 の S 1 と S 2 と同じであるので説明は省略する。

【0 1 5 9】

DNS サーバ 1 は、アドレス変換・フィルタリング装置 3 にてアドレス変換されたパケットを受信する。この時の名前解決要求パケットは「G l o b a l A (送信元アドレス)」, 「G l o b a l C (送信先アドレス)」, 及び「A. outside. com」を含む (S 3 3)。

【0 1 6 0】

DNS サーバ 1 は、名前解決要求パケットに含まれる名前「A. outside. com」を有する端末に対する通信の許可または不許可を判断する。即ち、DNS サーバ 1 は、通信許可ポートリスト 1 6 a に「A. outside. com」が存在するか否かを検索する。通信許可ポートリスト 1 6 a に「A. outside. com」が存在しなかった場合には、S 3 3 における名前解決要求パケットに対して名前解決が拒否される。即ち、DNS サーバ 1 は、アドレス変換・フィルタリング装置 3 に対して、問合せの回答として名前解決失敗 (E R R O R) を含む回答パケットを送信する (S 3 4)。

【0 1 6 1】

アドレス変換・フィルタリング装置 3 は、DNS サーバ 1 から受信した回答パケットの送信元アドレスと送信先アドレスをグローバル IP アドレスからプライベート IP アドレスへアドレス変換し、名前解決失敗 (E R R O R) を含む回答パケットを DNS サーバ 4 宛に送信する (S 3 5)。

【0 1 6 2】

DNS サーバ 4 は、回答パケットを受信すると、端末 2 に対し、名前解決要求に対する名前解決失敗 (E R R O R) を含む回答パケットを送信する (S 3 6)。

【0 1 6 3】

《G点におけるDNSサーバ1の動作フロー》

次に、図12におけるG点の処理について、図9を用いて説明する。図12のS100からS107間は、図3における通信許可時のプライベートIPアドレス網内からグローバルIPアドレス網への通信と同じである。従って、図12に示すような、名前により通信を拒否する場合の処理については、図9のS108から説明する。

【0164】

S108において、通信許可ポート検索部16は、通信許可ポートリスト16aから通信を許可するポート番号を検索した結果、ヒットしなかった場合には、問合せ元に対する回答は名前解決失敗となり、名前解決回答作成部20はDNSサーバ1の回答を作成する（S112）。図12に示す例では、問合せ先となる名前「A. outside. com」を検索キーとして、通信許可ポートリスト16aを検索し、通信を許可しているポート番号がない（ヒットしなかった）場合に、名前解決失敗となる。

【0165】

名前解決要求パケットに対する回答は、送信パケット作成部12でパケット化され、通信終端部10を経由して送信される（S111）。

【0166】

以上は、図12に示す名前による通信拒否時のプライベートIPアドレス網からグローバルIPアドレス網への通信において、図12のG点におけるDNSサーバ1の動作である。即ち、名前により通信が拒否された時のプライベートIPアドレス網からグローバルIPアドレス網への通信において、DNSサーバ1は、S100-S101-S104-S105-S106-S107-S108-S112-S111の順に動作する。

【0167】

本発明によれば、プライベートIPアドレス網からグローバルIPアドレス網への通信において、問合せ先となる端末の名前（例えば、ホスト名またはドメイン名）を用いて通信を拒否することができる。

【0168】

(4) ポートによる通信拒否時

次に、ポートによる通信拒否時のプライベート IP アドレス網内からグローバル IP アドレス網内への通信（図 5 の③に該当）について図 9、図 10、図 13 を用いて説明する。

【0169】

図 13 は、ポートにより通信を拒否する場合のプライベート IP アドレス網内からグローバル IP アドレス網内への通信を示す処理シーケンスである。ここでは、ポート番号として「ZZ」を持つサーバ 5 への通信を禁止する場合を想定して説明する。なお、図 13 は、図 3 の S 11 のパケットが拒否された場合に実行される処理であり、S 41 から S 50 間は、図 3 の S 1 から S 10 と同じであるので説明は省略し、S 51 から説明する。

【0170】

端末 2 は、DNS サーバ 4 から回答パケットを受信すると、問合せに対する回答が「Private E」であることを知る。即ち、端末 2 は、問合せた名前（A.outside.com）に対応する IP アドレスが「Private E」であることを知る。

【0171】

端末 2 は、サーバ 5 と通信を開始するために、データパケットを送信する（S 51）。この場合、データパケットのヘッダには「Private A（送信元 IP アドレス）」、「Private E（送信先 IP アドレス）」、「XX（送信元ポート番号）」、及び「ZZ（送信先ポート番号）」が設定される。

【0172】

端末 2 から送信されたデータパケットは、グレイゾーン上でアドレス変換・フィルタリング装置 3 を通過する。この時、アドレス変換・フィルタリング装置 3 は、データパケットの送信先ポート番号に基づいてフィルタリングを実施し、通信不可であると判断したデータパケットを破棄する。図 13 に示す例では、データパケットの送信先ポート番号「ZZ」に対してフィルタリングを実施する。本実施形態では、ポート番号「ZZ」に対して通信を禁止しているため、該パケットは破棄されている。

【0173】**《H点におけるアドレス変換・フィルタリング装置3の動作フロー》**

次に、図13におけるH点の処理について、図10を用いて説明する。図10のS120とS121は、図3における通信許可時のプライベートIPアドレス網内からグローバルIPアドレス網内への通信と同じであるため、説明は省略しS127から説明する。

【0174】

S127において、アドレス書換え・フィルタ部36は、アドレス書換え・フィルタデータベース35を検索する。即ち、データパケットの送信先IPアドレスをキーとしてデータベース35を検索し、ヒットした通信許可ポート番号とデータパケットの送信先ポート番号が一致しているか否かを判断する。図13に示す例では、データベース35に登録されている通信許可ポート番号とデータパケットの送信先ポート番号「ZZ」が一致していないと判断されたため、ミスヒットとなりパケットが破棄されている（S130）。

【0175】

以上は、図13に示すポートによる通信拒否時のプライベートIPアドレス網からグローバルIPアドレス網への通信において、図13のH点におけるアドレス変換・フィルタリング装置3の動作である。即ち、ポートにより通信が拒否された場合のプライベートIPアドレス網からグローバルIPアドレス網への通信において、アドレス変換・フィルタリング装置3は、S120-S121-S127-S130の順に動作する。

【0176】

本発明によれば、プライベートIPアドレス網からグローバルIPアドレス網への通信において、パケットがアドレス変換・フィルタリング装置3を通過する際、データパケットのポート番号に基づいて通信の可否を判断することができ、該パケットを通過させるか否かを決定することができる。

【0177】**〔グローバルIPアドレス網からプライベートIPアドレス網への通信〕**

次に、グローバルIPアドレス網からプライベートIPアドレス網への通信（

図5の②に該当) について図14を用いて説明する。

【0178】

図14は、グローバルIPアドレス網からプライベートIPアドレス網への通信を示す処理シーケンスである。図14に示す例では、端末2に名前“B. inside. fujitsu. com”が設定されている。

【0179】

まず、グローバルIPアドレス網(The Internet内のネットワーク)に収容されているサーバ5から端末2へパケットを転送する場合には、サーバ5は、端末2のIPアドレスを知るために、同一ネットワーク内に存在するDNSサーバ6宛に名前解決要求パケットを送信する(S61)。この場合、送信されるパケットは「Global D (送信元アドレス)」, 「Global C (送信先アドレス)」, 及び「B. inside. fujitsu. com (問合せ: 名前解決対象の端末2の名前)」となる。

【0180】

次に、DNSサーバ6は、自身が持つゾーンの情報では名前解決を行うことができないので、グレイゾーン上に位置するDNSサーバ1を送信先アドレスに設定した名前解決要求パケットを送信する(S62)。この時の名前解決要求パケットは「Global E (送信元アドレス)」, 「Global C (送信先アドレス)」, 及び「B. inside. fujitsu. com」を含む。

【0181】

DNSサーバ1は、DNSサーバ6から受信した名前解決要求パケットに基づいて通信の可否を判断する。本実施形態では、グローバルIPアドレス網からプライベートIPアドレス網への通信は禁止しているため、グローバルIPアドレス網からの名前解決要求は拒否される。即ち、DNSサーバ1は、DNSサーバ6に対して名前解決失敗(ERROR)を含む回答パケットを送信する(S63)。この場合、送信される回答パケットは「Global C (送信元アドレス)」, 「Global E (送信先アドレス)」, 及び「ERROR (回答)」を含む。

【0182】

DNSサーバ6は、回答パケットを受信すると、サーバ5に対し、名前解決要求パケットに対する回答パケットを送信する(S64)。この時、回答パケットは「Global E (送信元アドレス)」,「Global D (送信先アドレス)」,及び「ERROR (回答)」を含む。

【0183】

サーバ5は、DNSサーバ6から回答パケットを受信することで、プライベートIPアドレス網内に存在する端末2に対する名前解決が出来ないことを知る。

【0184】

《I点におけるDNSサーバ1の動作フロー》

次に、図14におけるI点の処理について、図9を用いて説明する。図9のS100からS105間は、図3におけるプライベートIPアドレス網からグローバルIPアドレス網への通信と同じである。従って、図14に示すグローバルIPアドレス網からプライベートIPアドレス網への通信については、図9のS106から説明する。

【0185】

S106において、名前解決部15は、名前解決要求パケットの問合せ元を示すIPアドレス(送信元アドレス)がグローバルIPアドレス網内のアドレスであり、且つパケットの問合せ先の名前がプライベートIPアドレス網内のサーバの名前である場合、即ち、図5の②に該当する場合には、名前解決要求を棄却する(S115)。

【0186】

以上は、図14に示すグローバルIPアドレス網からプライベートIPアドレス網への通信において、図14のI点におけるDNSサーバ1の動作である。即ち、グローバルIPアドレス網からプライベートIPアドレス網へ通信において、DNSサーバ1は、S100-S101-S104-S105-S106-S115の順に動作する。

【0187】

本発明によれば、DNSサーバ1は、グローバルIPアドレス網からプライベートIPアドレス網への通信を禁止(名前解決を拒否)することができ、通常の

DNSサーバとして機能することができる。

【0188】

〔グローバルIPアドレス網からグローバルIPアドレス網への通信〕

次に、グローバルIPアドレス網からグローバルIPアドレス網への通信（図5の④に該当）について図15を用いて説明する。

【0189】

図15は、グローバルIPアドレス網からグローバルIPアドレス網への通信を示す処理シーケンスである。図15に示す例では、グローバルIPアドレス網において、DNSサーバ6に“Global D”、サーバ5に“Global C（グローバルIPアドレス）”と“Port YY（ポート番号）”が設定されている。また、プライベートIPアドレス網において、端末2に“Global A（グローバルIPアドレス）”と“Port XX（ポート番号）”と“名前（B. DMZ. fujitsu. com）”が設定されている。また、グレイゾーン上において、DNSサーバ1に“Global B”が設定されている。

【0190】

まず、グローバルIPアドレス網（The Internet内のネットワーク）に収容されているサーバ5から端末2へパケットを転送する場合には、サーバ5は、端末2のIPアドレスを知るために、同一ネットワーク内に存在するDNSサーバ6に名前解決要求パケットを送信する（S71）。この場合、送信されるパケットは「Global C（送信元アドレス）」、「Global D（送信先アドレス）」、及び「B. DMZ. fujitsu. com（問合せ：名前解決対象の端末2の名前）」を含む。

【0191】

次に、DNSサーバ6は、自身が持つゾーンの情報では名前解決を行うことができないので、グレイゾーン上に位置するDNSサーバ1を送信先アドレスに設定した名前解決要求パケットを送信する（S72）。この時の名前解決要求パケットは「Global D（送信元アドレス）」、「Global B（送信先アドレス）」、及び「B. DMZ. fujitsu. com」を含む。

【0192】

DNSサーバ1は、DNSサーバ6から名前解決要求パケットを受信する。すると、名前解決要求パケットに含まれる名前に対応するIPアドレスを回答とする回答パケットをDNSサーバ6に返信する(S73)。この時、回答パケットは「Global B (送信元アドレス)」,「Global D (送信先アドレス)」,及び「Global A (回答:名前に対応するグローバルIPアドレス)」を含む。

【0193】

DNSサーバ6は、回答パケットを受信すると、サーバ5に対し、名前解決要求に対する回答パケットを送信する(S74)。この時、パケットは「Global D (送信元アドレス)」,「Global C (送信先アドレス)」,及び「Global A」を含む。

【0194】

名前解決要求パケットを送信したサーバ5は、DNSサーバ6から受信した回答パケットの内容から問合せに対する回答が「Global A」であることを知る。即ち、サーバ5は、問合せた名前(B.DMZ.fujitsu.com)に対応するIPアドレスが「Global A」であることを知る。

【0195】

端末2は、「Global A」を持つサーバ5と通信を開始するために、データパケットを送信する(S75)。この場合、データパケットのヘッダには「Global C (送信元アドレス)」,「Global A (送信先アドレス)」,「YY (送信元ポート番号)」,及び「XX (送信先ポート番号)」が設定される。

【0196】

端末2は、サーバ5からのデータパケットを受信するとサーバ5に対し、データパケットを返信する(S76)。この場合、データパケットのヘッダは「Global A (送信元アドレス)」,「Global C (送信先アドレス)」,「XX (送信元ポート番号)」,及び「YY (送信先ポート番号)」が設定される。

【0197】

《DNSサーバ1の動作フロー》

次に、図15のDNSサーバ1の動作について説明する。DNSサーバ1は、S100からS105間の動作は、図3に示されるプライベートIPアドレス網からグローバルIPアドレス網への通信と同じであるため説明は省略し、S106から説明する。

【0198】

S106において、パケットの問合せ先と問合せ元がいずれもグローバルIPアドレス網である場合、即ち、図5の④に該当する場合には、名前解決部15は、名前・アドレスデータベース（グローバル）15bを検索する（S107）。

【0199】

名前解決部15は、名前・アドレスデータベース（グローバル）15bを検索した結果、該当するIPアドレスがヒットした場合には、問合せ元への回答はヒットしたグローバルIPアドレスとなり、S112に進む。S107において、名前解決部15が、名前・アドレスデータベース（グローバル）15bを検索した結果、ミスヒットであった場合には、名前解決失敗としてS112に進む。

【0200】

S112では、名前解決回答作成部20は、DNSの回答を作成する。作成されたDNSの回答は、送信パケット作成部12でパケット化され、通信終端部10経由でネットワーク上に送信される（S111）。

【0201】

本発明によれば、DNSサーバ1は、グローバルIPアドレス網からグローバルIPアドレス網への通信に対して、グローバルIPアドレス網上に存在する通常のDNSサーバとして機能することができる。

【0202】

〔プライベートIPアドレス網からプライベートIPアドレス網への通信〕

次に、プライベートIPアドレス網からプライベートIPアドレス網への通信（図5の①に該当）について説明する。

【0203】

《DNSサーバ1の動作フロー》

プライベートIPアドレス網からプライベートIPアドレス網への通信は、図5の①に該当するため、DNSサーバ1の動作は、図15のグローバルIPアドレス網からグローバルIPアドレス網への通信（図5の④に該当）と同様となる。

【0204】

本発明によれば、DNSサーバ1は、プライベートIPアドレス網からプライベートIPアドレス網への通信に対して、プライベートIPアドレス網上に存在する通常のDNSサーバとして機能することができる。

【0205】

〈その他〉

本発明は、以下のように特定することができる。

（付記1） 通信元から送信される、通信先の名前に対応するアドレスの問合せを受信した場合に、通信元及び通信先がそれぞれ属するネットワーク種別に基づいて、通信元と通信先との間の通信の可否を判定する判定手段と、

前記判定手段の判定結果に基づいて、前記名前に対応する通信先のアドレスを通信元に回答するか否かを判定する第2判定手段と、

前記第2判定手段が通信先のアドレスを回答すると判定した場合に、通信先のアドレスを取得して通信元に回答する回答手段と、
を含む名前／アドレス変換装置。（1）

（付記2） 第1ネットワーク及び第2ネットワークから送信される、通信先の名前に対応する通信先のアドレスの問合せを受信する受信手段と、

前記問合せを送信した通信元、及び前記通信先がそれぞれ属するネットワークを識別する識別手段と、

前記通信元が前記第1ネットワークに属し且つ前記通信先が前記第2ネットワークに属する場合には、前記通信元に対して回答すべき前記通信先のアドレスを検索する検索手段と、

前記通信先のアドレスを含む回答を送出する送出手段とを含み、

前記送出手段は、前記通信元が前記第2ネットワークに属し且つ前記通信先が

前記第 1 ネットワークに属する場合には、前記通信先のアドレスを含む回答を送出しない

名前／アドレス変換装置。(2)

(付記 3) 前記送出手段は、前記第 1 ネットワークに属する通信元と前記第 2 ネットワークに属する通信先との間での通信で使用が許可されたアプリケーションがない場合には、前記通信元へ前記通信先のアドレスを回答しない

付記 2 記載の名前／アドレス変換装置。(3)

(付記 4) 前記第 1 ネットワークに属する通信元に相当する第 1 端末に対して前記第 2 ネットワークに属する通信先に相当する第 2 端末のアドレスが回答される場合に、前記第 1 ネットワークと前記第 2 ネットワークとの間を転送されるデータを受信して通過が許可されたデータのみを通過させるとともに、前記第 1 ネットワークと前記第 2 ネットワークとの間のアドレス変換を行う中継装置に対し、前記第 1 端末と前記第 2 端末との間を転送されるデータを通過させるための通過情報を通知する通知手段をさらに含む

付記 2 又は 3 記載の名前／アドレス変換装置。(4)

(付記 5) 前記通知手段は、前記中継装置が前記第 2 端末から送信されるデータを通過させるときに、このデータに送信元アドレスとして付加された前記第 2 端末の前記第 2 ネットワークにおけるアドレスを前記第 1 ネットワークのアドレスに変換するために、前記第 2 端末に対して仮想的に割り当てられる前記第 1 ネットワークのアドレスと前記第 2 端末の前記第 2 ネットワークにおけるアドレスとを含む通過情報とを前記中継装置に通知し、

前記送出手段は、前記第 1 端末が前記第 2 端末宛のデータに前記第 2 端末の前記第 1 ネットワークにおけるアドレスを送信先アドレスとして付加して送信し、且つ前記中継装置が前記第 2 端末宛のデータを通過させるときにこのデータに付加された送信先アドレスを前記第 2 端末の前記第 2 ネットワークにおけるアドレスに変換するために、前記第 2 端末の前記第 1 ネットワークにおけるアドレスを含む回答を送出する

付記 4 記載の名前／アドレス変換装置。(5)

(付記 6) 前記通知手段は、前記中継装置が前記第 1 端末と前記第 2 端末との

間での利用が許可されたアプリケーションに基づくデータのみを通過させるために、前記第 1 端末と前記第 2 端末との間の通信での利用が許可されたアプリケーションに係る情報をさらに含む通過情報を前記中継装置に通知する

付記 4 又は 5 記載の名前／アドレス変換装置。

(付記 7) 前記通知手段は、前記送出手段が前記第 2 端末のアドレスを送出する前に、前記通過情報を前記中継装置に通知する

付記 4 ～ 6 のいずれかに記載の名前／アドレス変換装置。

(付記 8) 名前／アドレス変換装置として機能するコンピュータが、
通信元から送信される、通信先の名前に対応するアドレスの問合せを受信した場合に、通信元及び通信先がそれぞれ属するネットワーク種別に基づいて、通信元と通信先との間の通信の可否を判定し、

前記判定ステップの判定結果に基づいて、前記名前に対応する通信先のアドレスを通信元に回答するか否かを判定し、

前記第 2 判定ステップが通信先のアドレスを回答すると判定した場合に、通信先のアドレスを取得して通信元に回答することを含む名前／アドレス変換方法。

(付記 9) 名前／アドレス変換装置として機能するコンピュータが、
第 1 ネットワーク及び第 2 ネットワークから送信される、通信先の名前に対応する通信先のアドレスの問合せを受信し、

前記問合せを送信した通信元、及び前記通信先がそれぞれ属するネットワークを識別し、

前記通信元が前記第 1 ネットワークに属し且つ前記通信先が前記第 2 ネットワークに属する場合には、前記通信元に対して回答すべき前記通信先のアドレスを検索し、

前記通信先のアドレスを含む回答を送出し、
前記通信元が前記第 2 ネットワークに属し且つ前記通信先が前記第 1 ネットワークに属する場合には、前記通信先のアドレスを含む回答を送出しない
ことを含む名前／アドレス変換方法。

(付記 1 0) 前記コンピュータは、

前記第 1 ネットワークに属する通信元と前記第 2 ネットワークに属する通信先との間での通信で使用が許可されたアプリケーションがない場合には、前記通信元へ前記通信先のアドレスを回答しない

付記 9 記載の名前/アドレス変換方法。

(付記 1 1) 前記コンピュータは、

前記第 1 ネットワークに属する通信元に相当する第 1 端末に対して前記第 2 ネットワークに属する通信先に相当する第 2 端末のアドレスが回答される場合に、前記第 1 ネットワークと前記第 2 ネットワークとの間を転送されるデータを受信して通過が許可されたデータのみを通過させるとともに、前記第 1 ネットワークと前記第 2 ネットワークとの間のアドレス変換を行う中継装置に対し、前記第 1 端末と前記第 2 端末との間を転送されるデータを通過させるための通過情報を通知する

ことをさらに含む付記 9 又は 1 0 記載の名前/アドレス変換方法。

(付記 1 2) 前記コンピュータは、

前記中継装置が前記第 2 端末から送信されるデータを通過させるときに、このデータに送信元アドレスとして付加された前記第 2 端末の前記第 2 ネットワークにおけるアドレスを前記第 1 ネットワークのアドレスに変換するために、前記第 2 端末に対して仮想的に割り当てられる前記第 1 ネットワークのアドレスと前記第 2 端末の前記第 2 ネットワークにおけるアドレスとを含む通過情報とを前記中継装置に通知し、

前記第 1 端末が前記第 2 端末宛のデータに前記第 2 端末の前記第 1 ネットワークにおけるアドレスを送信先アドレスとして付加して送信し、且つ前記中継装置が前記第 2 端末宛のデータを通過させるときにこのデータに付加された送信先アドレスを前記第 2 端末の前記第 2 ネットワークにおけるアドレスに変換するために、前記第 2 端末の前記第 1 ネットワークにおけるアドレスを含む回答を送出する

付記 1 1 記載の名前/アドレス変換方法。

(付記 1 3) 前記コンピュータは、

前記中継装置が前記第 1 端末と前記第 2 端末との間での利用が許可されたアプ

リケーションに基づくデータのみを通過させるために、前記第 1 端末と前記第 2 端末との間の通信での利用が許可されたアプリケーションに係る情報をさらに含む通過情報を前記中継装置に通知する

付記 1 1 又は 1 2 記載の名前/アドレス変換方法。

(付記 1 4) 前記コンピュータは、

前記第 2 端末のアドレスを送出する前に、前記通過情報を前記中継装置に通知する

付記 1 1 ～ 1 3 のいずれかに記載の名前/アドレス変換方法。

(付記 1 5) コンピュータを名前/アドレス変換装置として機能させるプログラムまたはこのプログラムを記録した記録媒体であって、

通信元から送信される、通信先の名前に対応するアドレスの問合せを受信した場合に、通信元及び通信先がそれぞれ属するネットワーク種別に基づいて、通信元と通信先との間の通信の可否を判定する判定ステップと、

前記判定ステップの判定結果に基づいて、前記名前に対応する通信先のアドレスを通信元に回答するか否かを判定する第 2 判定ステップと、

前記第 2 判定ステップが通信先のアドレスを回答すると判定した場合に、通信先のアドレスを取得して通信元に回答する回答ステップと、
を前記コンピュータに実行させるプログラムまたはこのプログラムを記録した記録媒体。

(付記 1 6) コンピュータを名前/アドレス変換装置として機能させるプログラムまたはこのプログラムを記録した記録媒体であって、

第 1 ネットワーク及び第 2 ネットワークから送信される、通信先の名前に対応する通信先のアドレスの問合せを受信する受信ステップと、

前記問合せを送信した通信元、及び前記通信先がそれぞれ属するネットワークを識別する識別ステップと、

前記通信元が前記第 1 ネットワークに属し且つ前記通信先が前記第 2 ネットワークに属する場合には、前記通信元に対して回答すべき前記通信先のアドレスを検索する検索ステップと、

前記通信先のアドレスを含む回答を送出する送出ステップとを含み、

前記通信元が前記第 2 ネットワークに属し且つ前記通信先が前記第 1 ネットワークに属する場合には、前記通信先のアドレスを含む回答を送出しないステップと、
を前記コンピュータに実行させるプログラムまたはこのプログラムを記録した記録媒体。

(付記 1 7) 前記第 1 ネットワークに属する通信元と前記第 2 ネットワークに属する通信先との間での通信で使用が許可されたアプリケーションがない場合には、前記通信元へ前記通信先のアドレスを回答しないことを判断するステップを前記コンピュータに実行させる付記 1 6 記載のプログラムまたはこのプログラムを記録した記録媒体。

(付記 1 8) 前記第 1 ネットワークに属する通信元に相当する第 1 端末に対して前記第 2 ネットワークに属する通信先に相当する第 2 端末のアドレスが回答される場合に、前記第 1 ネットワークと前記第 2 ネットワークとの間を転送されるデータを受信して通過が許可されたデータのみを通過させるとともに、前記第 1 ネットワークと前記第 2 ネットワークとの間のアドレス変換を行う中継装置に対し、前記第 1 端末と前記第 2 端末との間を転送されるデータを通過させるための通過情報を通知する通知ステップを、

さらに前記コンピュータに実行させる付記 1 6 又は 1 7 記載のプログラムまたはこのプログラムを記録した記録媒体。

(付記 1 9) 前記中継装置が前記第 2 端末から送信されるデータを通過させるときに、このデータに送信元アドレスとして付加された前記第 2 端末の前記第 2 ネットワークにおけるアドレスを前記第 1 ネットワークのアドレスに変換するために、前記第 2 端末に対して仮想的に割り当てられる前記第 1 ネットワークのアドレスと前記第 2 端末の前記第 2 ネットワークにおけるアドレスとを含む通過情報とを前記中継装置に通知するステップと、

前記第 1 端末が前記第 2 端末宛のデータに前記第 2 端末の前記第 1 ネットワークにおけるアドレスを送信先アドレスとして付加して送信し、且つ前記中継装置が前記第 2 端末宛のデータを通過させるときにこのデータに付加された送信先アドレスを前記第 2 端末の前記第 2 ネットワークにおけるアドレスに変換するため

に、前記第2端末の前記第1ネットワークにおけるアドレスを含む回答を送出するステップとを、

前記コンピュータに実行させる付記18記載のプログラムまたはこのプログラムを記録した記録媒体。

(付記20) 前記中継装置が前記第1端末と前記第2端末との間での利用が許可されたアプリケーションに基づくデータのみを通過させるために、前記第1端末と前記第2端末との間の通信での利用が許可されたアプリケーションに係る情報をさらに含む通過情報を前記中継装置に通知するステップを、
前記コンピュータに実行させる付記18又は19記載のプログラムまたはこのプログラムを記録した記録媒体。

(付記21) 前記送出ステップが前記第2端末のアドレスを送出する前に、前記通過情報を前記中継装置に通知するステップを、
前記コンピュータに実行させる付記18～20のいずれかに記載のプログラムまたはこのプログラムを記録した記録媒体。

【0206】

【発明の効果】

本発明によれば、プロキシサーバを用いることなく、IPネットワーク間の境界にあるDNSサーバとアドレス変換装置を連携させることにより、異なるIPネットワーク空間にまたがる通信を実現することが可能となる。

【図面の簡単な説明】

【図1】 従来技術であるDNSの仕組みを示すDNSツリー図である。

【図2】 従来のプライベートIPアドレス網からグローバルIPアドレス網間通信におけるDNSのフローを示す図である。

【図3】 本発明の実施形態における通信許可時のプライベートIPアドレス網からグローバルIPアドレス網への通信を示す図である。

【図4】 プライベートIPアドレス網に対するグローバルIPアドレス網の見せ方を示す図である。

【図5】 名前解決要求の問合せ元に応じたDNSサーバの回答を示す図である。

【図 6】 本発明の実施形態における D N S サーバのシステム構成を示す図である。

【図 7】 本発明の実施形態におけるアドレス変換・フィルタリング装置のシステム構成を示す図である。

【図 8】 本発明の実施形態におけるパケットのデータ構造を示す図である。

【図 9】 本発明の実施形態における D N S サーバの動作を示すフローチャートである。

【図 1 0】 本発明の実施形態におけるアドレス変換・フィルタリング装置の動作を示すフローチャートである。

【図 1 1】 本発明の実施形態におけるプライベート I P アドレスの返却処理を示す図である。

【図 1 2】 本発明の実施形態における名前による通信拒否時のプライベート I P アドレス網からグローバル I P アドレス網への通信を示す図である。

【図 1 3】 本発明の実施形態におけるポートによる通信拒否時のプライベート I P アドレス網からグローバル I P アドレス網への通信を示す図である。

【図 1 4】 本発明の実施形態におけるグローバル I P アドレス網からプライベート I P アドレス網への通信を示す図である。

【図 1 5】 本発明の実施形態におけるグローバル I P アドレス網からグローバル I P アドレス網への通信を示す図である。

【符号の説明】

1, 4, 6	D N S サーバ
2, 5	端末
3	アドレス変換・フィルタリング装置
7	L 2 - S W
8	ルータ
1 0	通信終端部
1 1	受信識別部
1 2	送信パケット作成部

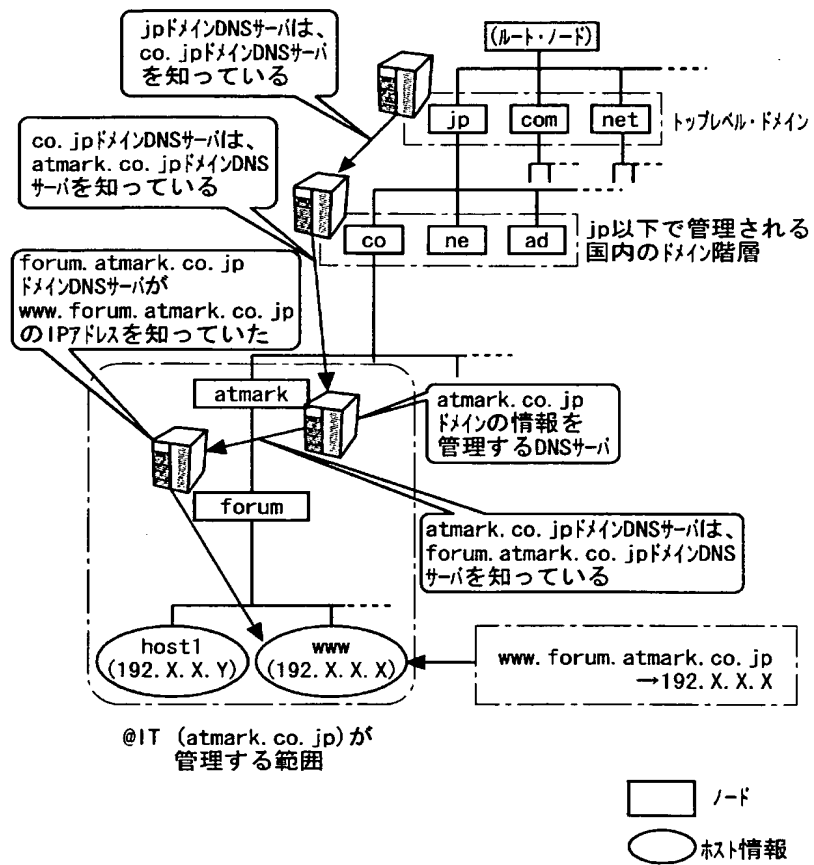
1 3	名前解決要求問合せ元識別部
1 4	名前解決要求問合せ先識別部
1 5	名前解決部
1 5 a, 1 5 b	名前・アドレスデータベース
1 6	通信許可ポート検索部
1 6 a	通信許可ポートリスト
1 7	アドレス割当部
1 8	アドレス返却部
1 9	アドレスプール管理部
1 9 a	アドレスプールリスト
2 0	名前解決回答作成部
2 1	アドレス通知作成部
3 1	通信終端部
3 2	受信識別部
3 3	送信パケット作成部
3 4	フィルタ書換え部
3 5	アドレス書換え・フィルタデータベース
3 6	アドレス書換え・フィルタ部
3 7	タイマ部
3 8	設定完了通知部
3 9	N A T 部
4 0	返却通知作成部
1 0 0	パケット

【書類名】

図面

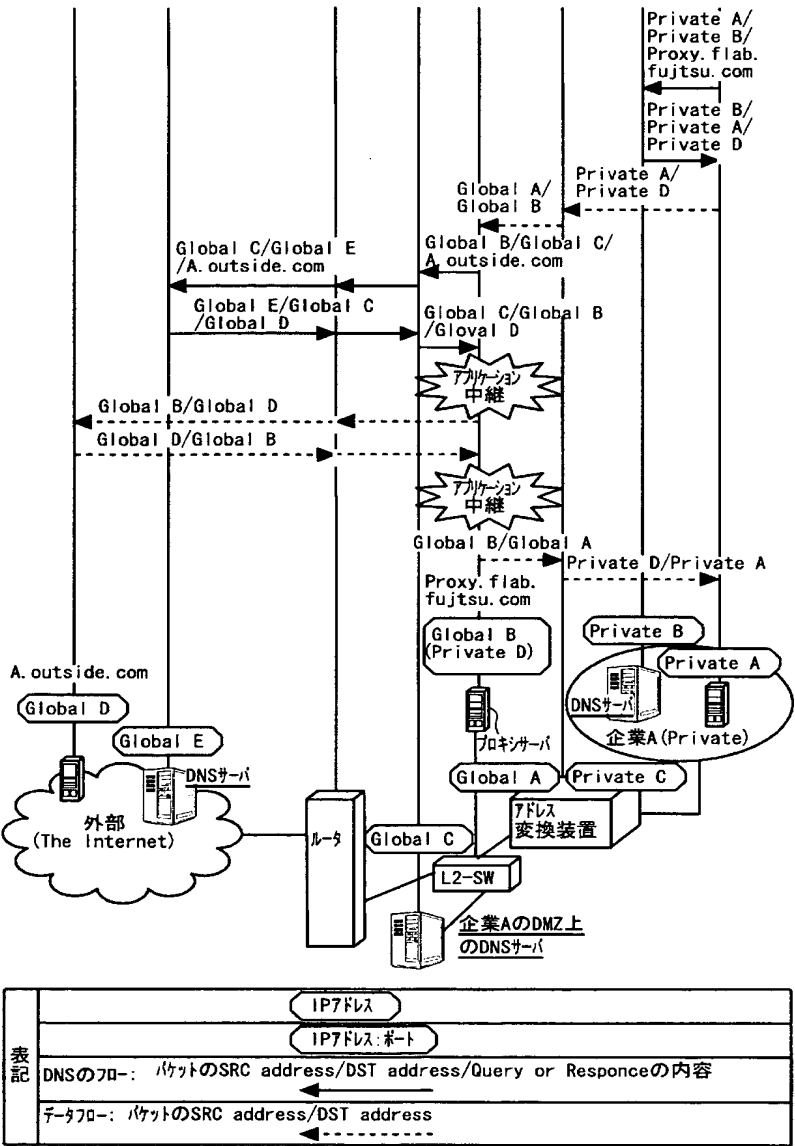
【図 1】

DNSツリー図



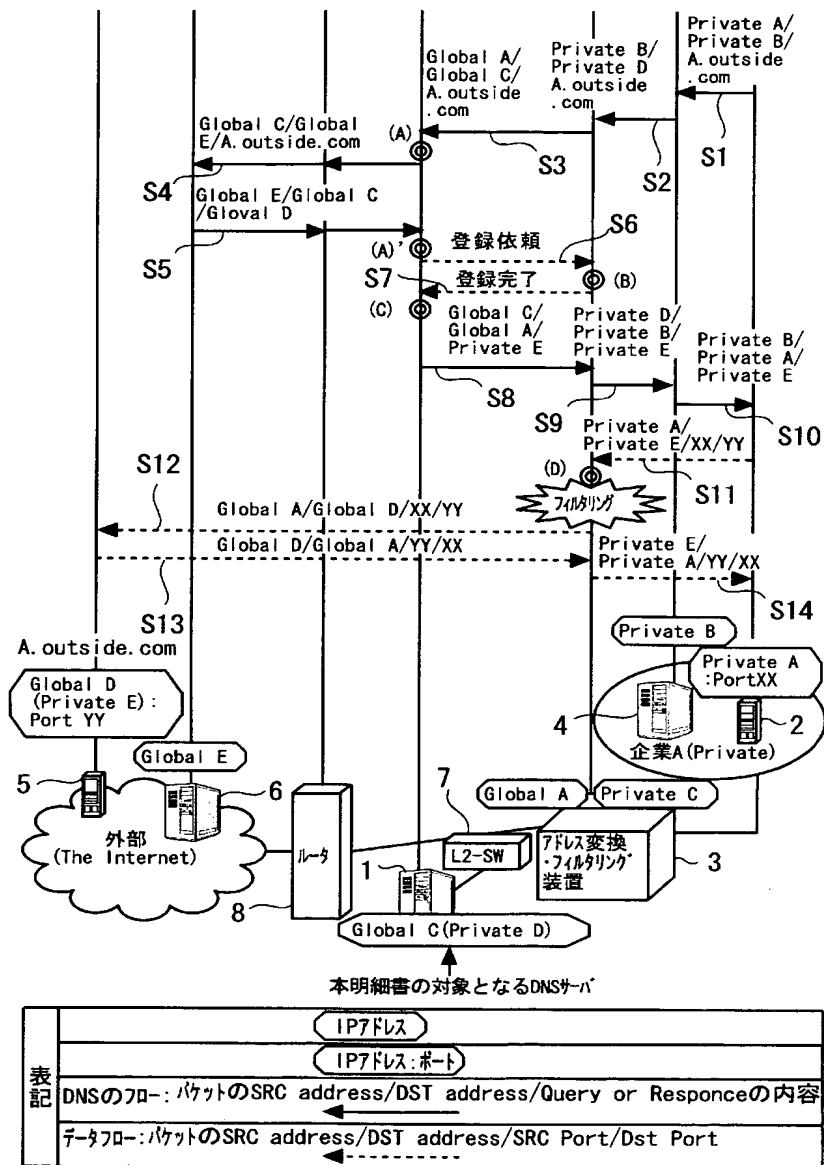
【図 2】

プライベートIP網からグローバルIP網間通信におけるDNSのフロー(従来)



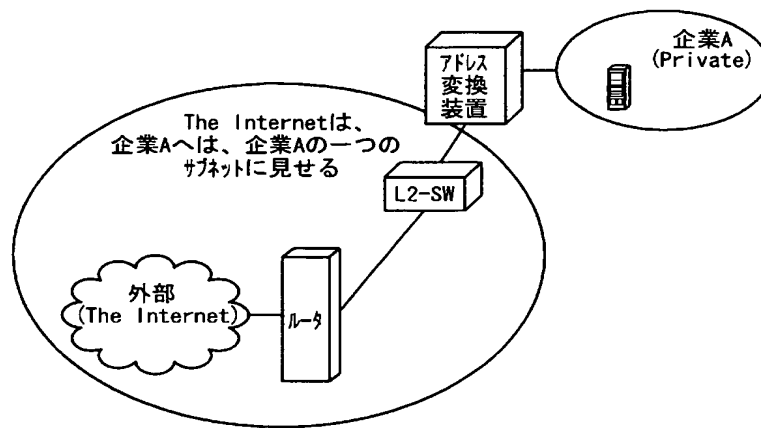
【図 3】

プライベートIPアドレス網内からグローバルIPアドレス網への通信フロー図(通信許可時)



【図 4】

プライベートIPアドレス網へのグローバルIPアドレス網の見せ方

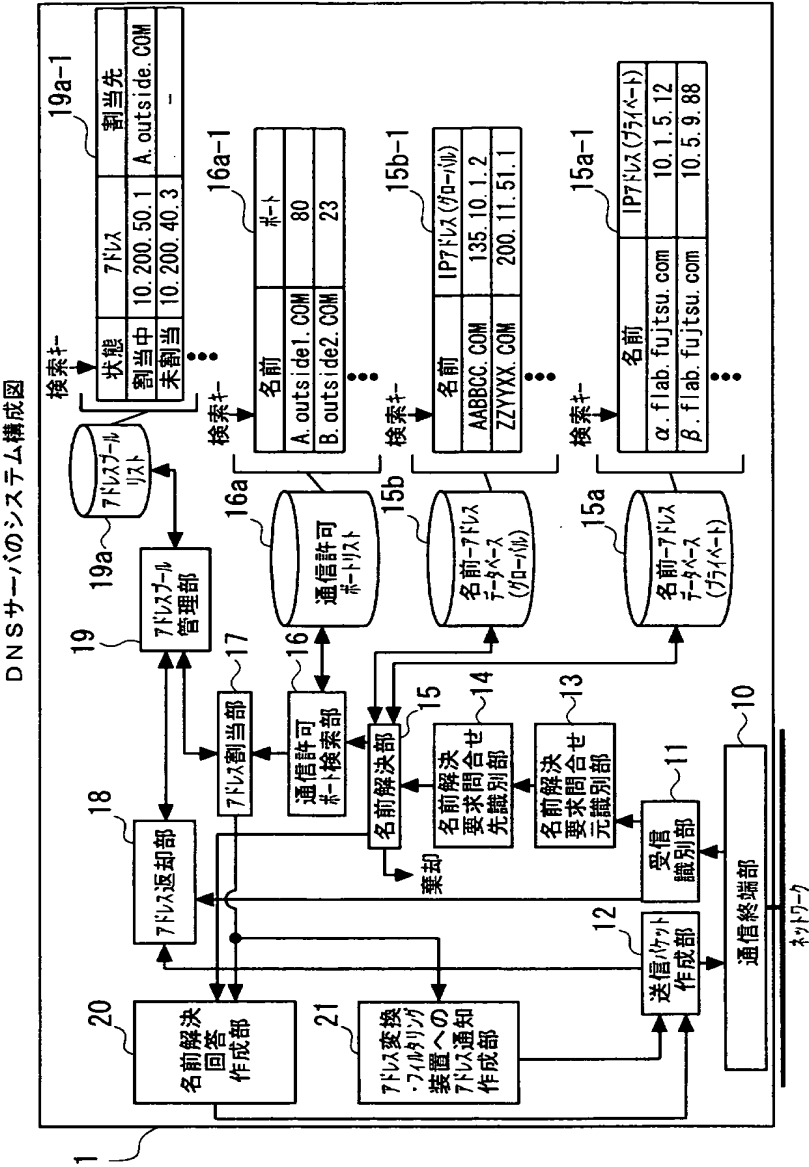


【図 5】

名前解決要求の問合せ元に応じたDNSサーバの回答

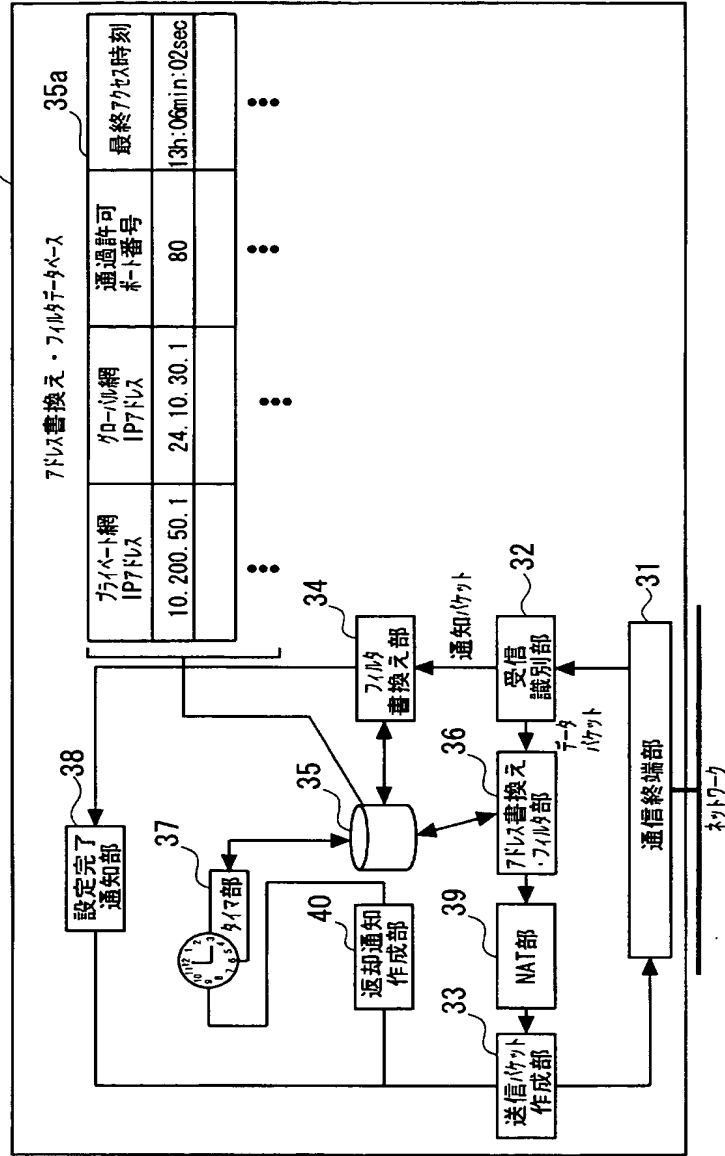
名前解決要求 の問合せ元 解決する 名前の端末位置	プライベートIPアドレス網	グローバルIPアドレス網
プライベートIPアドレス網	①通常のプライベートIP アドレス網上のDNSサーバ として動作	②名前解決要求棄却
グローバルIPアドレス網	③接続可否を判断 の上、回答	④通常のグローバルIP アドレス網上のDNSサーバ として動作

【図 6】



【図 7】

アドレス変換・フィルタリング装置のシステム構成図

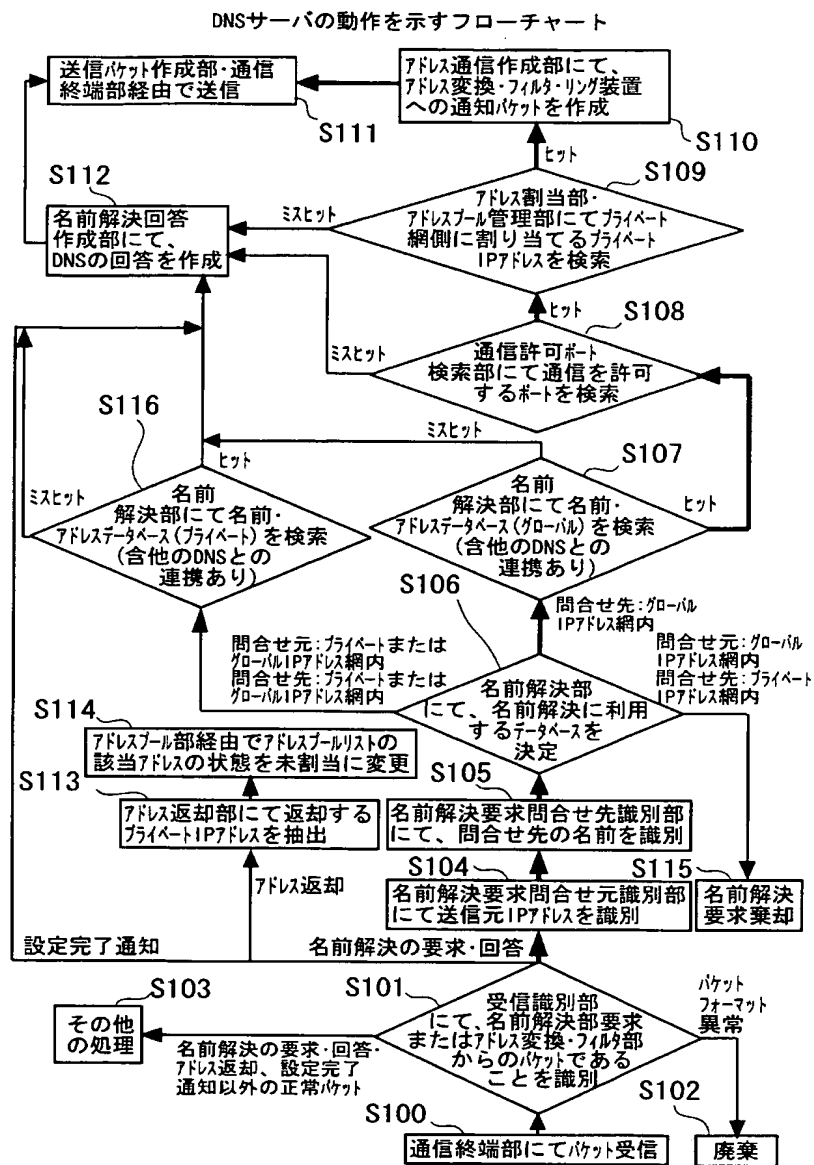


【図 8】

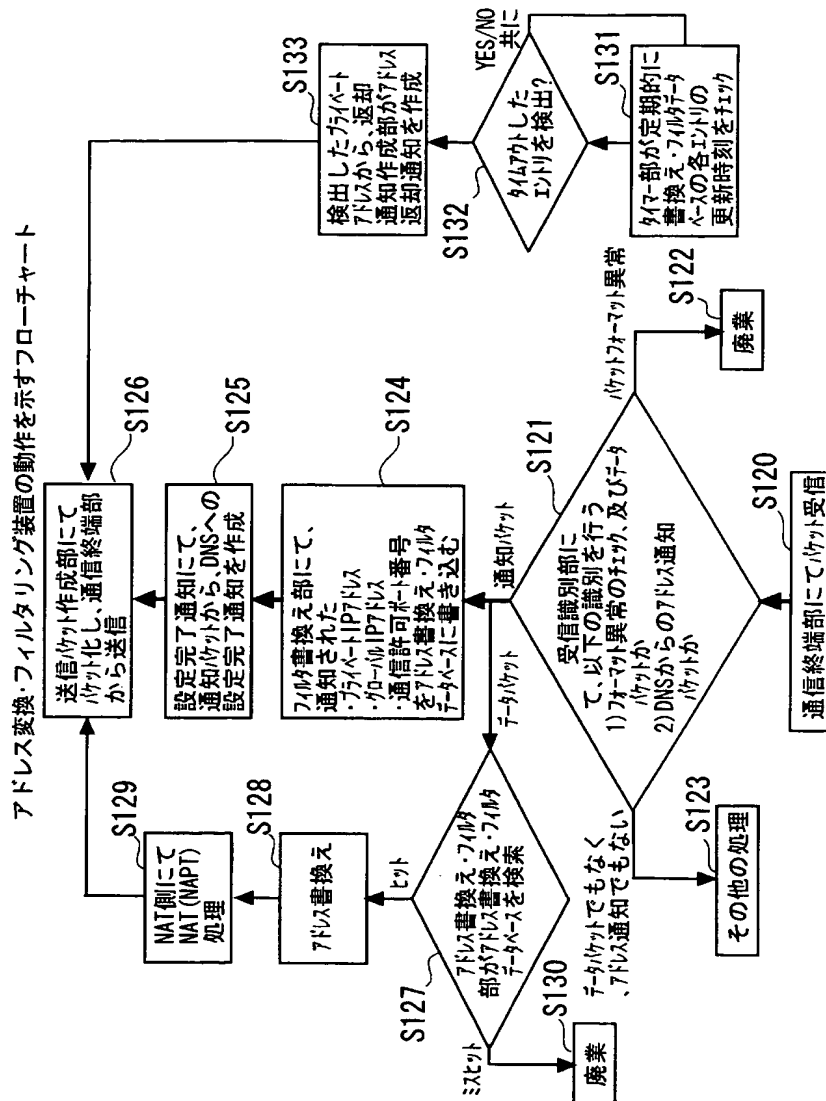
パケットのデータ構造(ヘッダ部)

63	56155	48147	40139	32131	24123	16115	817	0
ver	Header Length	TOS	Total Length	ID		Fragment		
MAC S. A [31:0]				Frame Type/Frame Length		ver	Header Length	TOS
TTL	Protocol	Checksum		送信元アドレス				
送信先アドレス				送信元ポート		送信先ポート		

【図 9】



【図 10】



【図 1 1】

プライベートIPアドレスの返却時のフロー

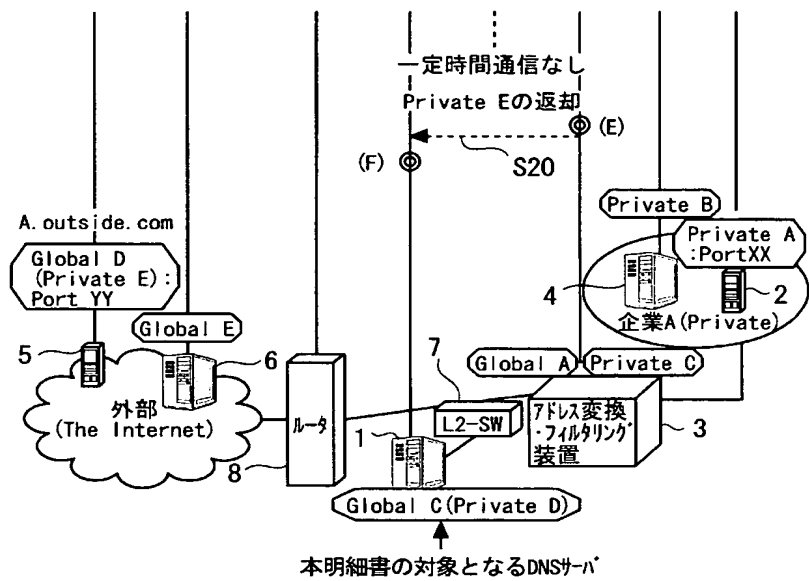
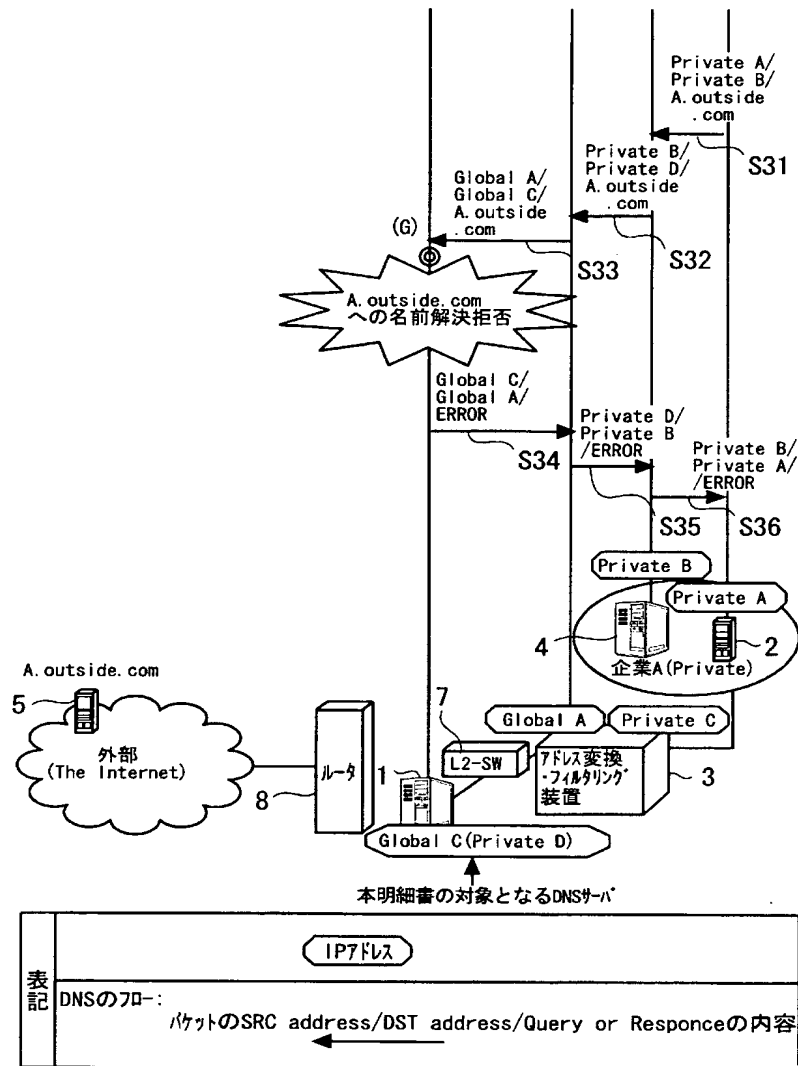


表 記	IPアドレス
	IPアドレス:ポート
	データフロー: ←-----

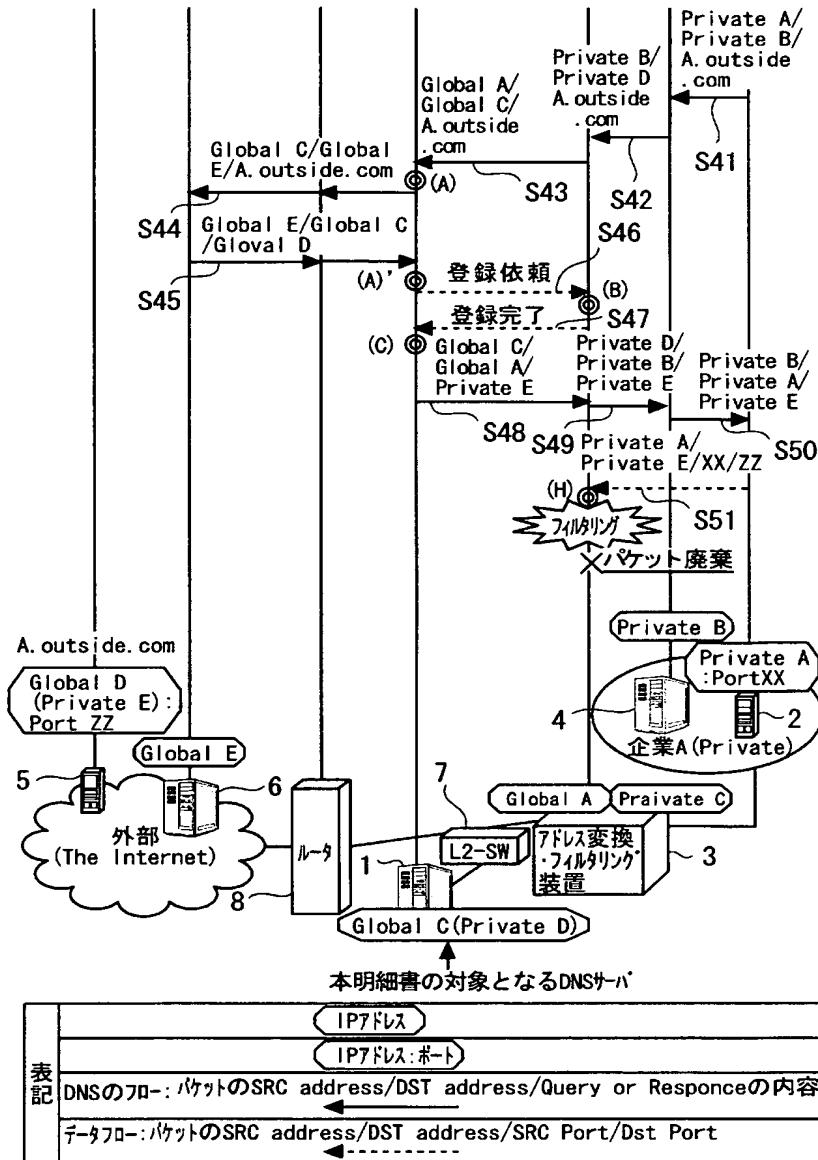
【図 12】

プライベートIPアドレス内網からグローバルIPアドレス網への通信
(名前による通信拒否時)



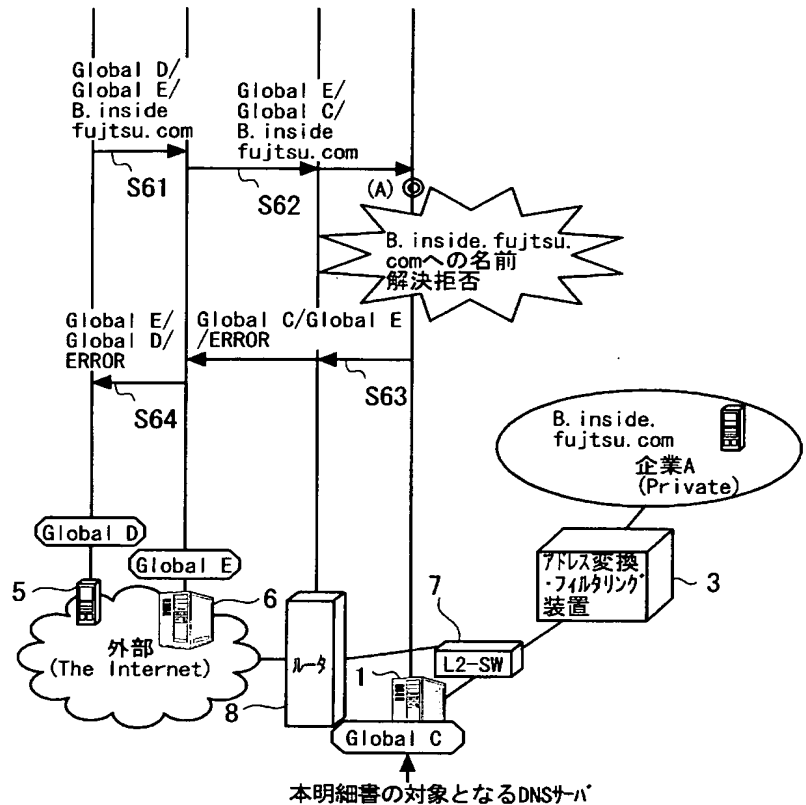
【図 13】

プライベートIPアドレス網からグローバルIPアドレス網内への通信
(ポートによる通信拒否時)



【図 14】

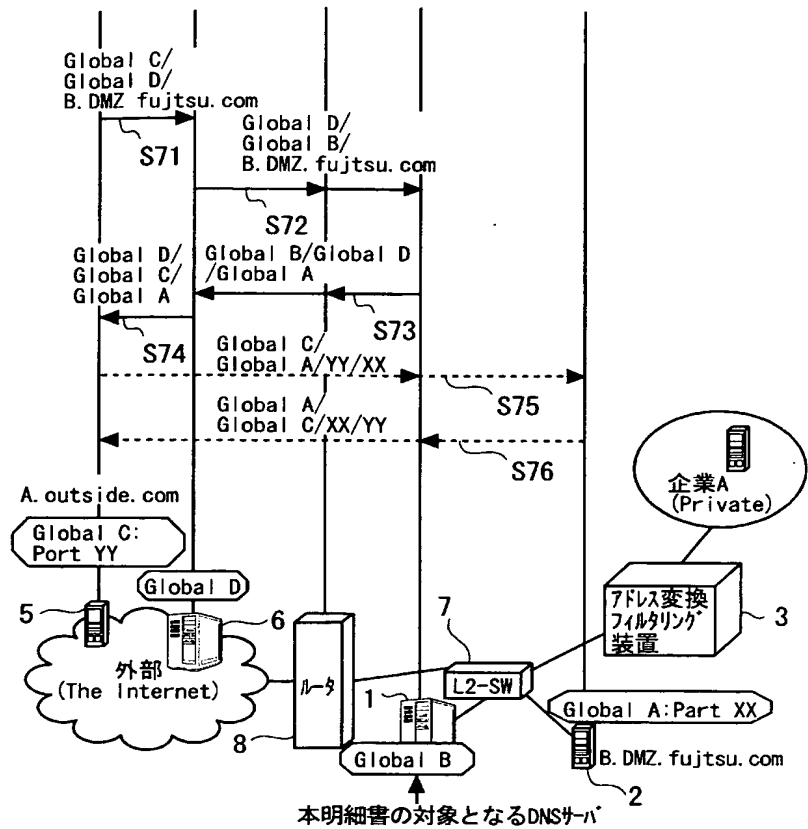
グローバルIPアドレス網からプライベートIPアドレス網への通信



表記	IPアドレス
	DNSのフォーマット: パケットのSRC address/DST address/Query or Responseの内容

【図 15】

グローバルIPアドレス網からグローバルIPアドレス網への通信



表記	IPアドレス
	IPアドレス:ポート
	DNSのフロー: パケットのSRC address/DST address/Query or Responceの内容
	データフロー: パケットのSRC address/DST address/SRC Port/Dst Port

【書類名】 要約書

【要約】

【課題】 異なる IP ネットワーク間にまたがる通信をプロキシサーバを用いることなく実現することができる装置や方法を提供する。

【解決手段】 名前／アドレス変換装置は、通信元から送信される、通信先の名前に対応するアドレスの問合せを受信した場合に、通信元及び通信先がそれぞれ属するネットワーク種別に基づいて、通信元と通信先との間の通信の可否を判定する判定手段と、上記判定手段の判定結果に基づいて、上記名前に対応する通信先のアドレスを通信元に回答するか否かを判定する第 2 判定手段と、上記第 2 判定手段が通信先のアドレスを回答すると判定した場合に、通信先のアドレスを取得して通信元に回答する回答手段とを含む。

【選択図】 図 6

特願 2 0 0 3 - 0 9 1 2 9 3

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 5 2 2 3]

1. 変更年月日

1 9 9 6 年 3 月 2 6 日

[変更理由]

住所変更

住 所

神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号

氏 名

富士通株式会社